Symantec AntiVirus™ Corporate Edition Руководство администратора



Symantec AntiVirus™ Corporate Edition Руководство администратора

Авторские права

Версия документации 1a

Товарные знаки

Напечатано в Ирландии.

10 9 8 7 6 5 4 3 2 1

Оглавление

Раздел 1 Управление Symantec AntiVirus Corporate Edition

Глава 1 Управление Symantec AntiVirus Corporate Edition

Раздел 1

Управление Symantec AntiVirus Corporate Edition

Глава 1

Управление Symantec AntiVirus Corporate Edition

Эта глава содержит следующие разделы:

Сведения об управлении Symantec AntiVirus Corporate Edition

С помощью Symantec System Center вы можете выполнять такие операции управления Symantec AntiVirus Corporate Edition, как установка антивирусной защиты на рабочих станциях и сетевых серверах, обновление описаний вирусов, а также управление серверами и клиентами Symantec AntiVirus Corporate Edition. Помимо Symantec System Center для настройки клиентов Symantec AntiVirus Corporate Edition могут также применяться файлы конфигурации (Grc.dat). Файлы конфигурации можно применять, например, для удаленной настройки подключенных к сети компьютеров с помощью инструментов независимых поставщиков.

Дополнительная информация о применении файлов конфигурации приведена в книге «*Symantec AntiVirus Corporate Edition: Справочник*».

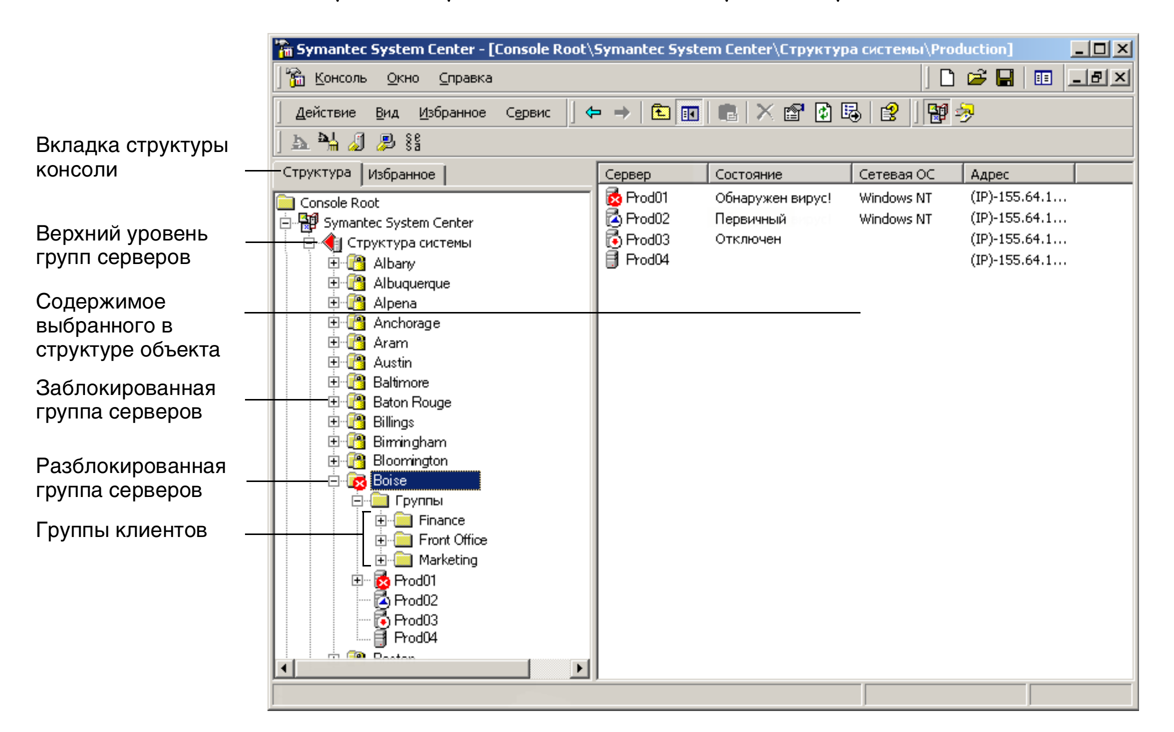
Управление с помощью Symantec System Center

При запуске Symantec System Center показывает структуру системы, включающую группы серверов, клиентов, а также отдельные серверы. Эта структура отображается в виде дерева, отдельные ветви которого можно разворачивать и сворачивать. Структура системы определяет верхний уровень иерархии, включающий все группы серверов и клиентов.

Примечание: Структура системы остается пустой до тех пор, пока вы не установите по крайней мере один сервер Symantec AntiVirus Corporate Edition.

Запуск Symantec System Center

- На панели задач Windows выберите команды **Пуск** > **Программы** > **Symantec System Center Console** > **Symantec System Center Console**.



Режимы просмотра консоли

Каждый устанавливаемый модуль управления продуктом добавляет в Symantec System Center новый режим просмотра. Например, после установки модуля управления Symantec AntiVirus Corporate Edition появляется режим Symantec AntiVirus, в котором имеются поля, относящиеся к программе Symantec AntiVirus Corporate Edition, например, «Последний осмотр» и «Описания».

Столбцы, представленные в правом окне, изменяются в соответствии с выбранным режимом. Например, если выбрана структура системы, то в режиме вида консоли по умолчанию будут показаны следующие столбцы:

- Имя
- Состояние
- Первичный сервер
- Проверка доступа

Табл. 1-1 содержит список столбцов, отображаемых в режиме просмотра Symantec AntiVirus.

Табл. 1-1 Столбцы, отображаемые в режиме просмотра Symantec AntiVirus

Объект, выбранный в левом окне	Столбцы, показанные в правом окне
Значок структуры системы	■ Группа серверов ■ Состояние ■ Общие описания ■ Новейшие описания ■ Состояние обновлений сервера
Значок группы серверов	■ Сервер ■ Тип ■ Состояние ■ Последний осмотр ■ Описания ■ Версия ■ Сканер ■ Адрес ■ Состояние обновлений клиентов
Значок группы клиентов	■ Имя группы ■ Дата изменения конфигурации ■ Количество клиентов
Значок группы клиентов или серверов	■ Клиент ■ Пользователь ■ Состояние ■ Тип ОС ■ Адрес ■ Группа ■ Сервер ■ Время последнего контрольного сеанса

Режимы просмотра консоли

Если не выбран другой режим, то Symantec System Center показывает вид консоли по умолчанию. Список доступных режимов просмотра зависит от установленных управляемых продуктов Symantec AntiVirus Corporate Edition.

Изменение режима просмотра консоли

1 В левой части окна консоли Symantec System Center разверните объект **Структура системы**.

2 В меню «Вид» выберите режим просмотра в списке, показанном в нижней части меню.

Сохранение параметров консоли

При выходе из консоли на экране появляется запрос о сохранении настроек консоли для Symantec System Center.

Сохранение настроек

◆ Выполните одно из следующих действий:

- Для того чтобы при следующем запуске Symantec System Center был выбран текущий режим просмотра консоли, нажмите кнопку «**Да**».
- Для того чтобы при следующем запуске Symantec System Center был выбран последний сохраненный режим просмотра консоли, нажмите кнопку «**Нет**».

  Выбор варианта «Нет» может привести к потере внесенных в настройку изменений. Например, если были изменены параметры подключенного сервера изолятора, то выбор варианта «**Нет**» при выходе из консоли MMC может привести к тому, что измененные параметры сервера изолятора не будут сохранены.

Примечание: Если в системе есть более новая версия MMC, то для сохранения параметров при выходе из консоли Symantec System Center может потребоваться перейти к новой версии.

Описание значков Symantec System Center

В программе Symantec System Center для представления различных состояний компьютеров с управляемыми программами Symantec используются значки. Например, если группа серверов представлена значком с изображением закрытого замка, значит, для получения доступа к настройке или запуску осмотров на компьютерах, входящих в эту группу, ее необходимо разблокировать с помощью пароля.

Табл. 1-2 содержит список значков Symantec System Center.

Табл. 1-2 Symantec System Center

Значок	Описание значка
	Объект верхнего уровня, представляющий структуру системы, содержащую все группы серверов.
	Разблокированная группа серверов или клиентов. Сравните этот значок со значком блокированной группы серверов. В целях обеспечения безопасности все группы серверов при запуске Symantec System Center по умолчанию блокируются.
	Заблокированная группа серверов Для получения доступа к компьютерам, входящих в группу, а также для изменения их параметров и выполнения обновлений и осмотров необходимо ввести пароль.
	Группа серверов, в которой обнаружены неполадки, требующие устранения. Например, в группе отсутствует первичный сервер или один из серверов заражен вирусом.
	Сервер Symantec AntiVirus Corporate Edition. Это может быть сервер Windows NT/2000 или NetWare. Сравните этот значок со следующим, представляющим первичный сервер группы.
	Первичный сервер Symantec AntiVirus Corporate Edition. Это может быть сервер Windows NT/2000 или NetWare.
	Недоступный сервер Symantec AntiVirus Corporate Edition. Этот значок появляется в случае сбоя связи между сервером Symantec AntiVirus Corporate Edition и консолью Symantec System Center. Сбой связи может быть вызван различными причинами. Например, не работает система сервера, удалено программное обеспечение Symantec или имеется неисправность в сети на участке между консолью и сервером.
	На компьютере, на котором работает сервер Symantec AntiVirus Corporate Edition, обнаружен вирус.
	Клиент Symantec AntiVirus Corporate Edition, работающий на компьютере под управлением Windows 95/98/Me, либо Windows NT/2000/XP Home Edition или Professional. Компьютер Windows 95, применяющий устаревшую версию клиента Symantec AntiVirus . При выборе такого компьютера будут показаны только параметры, относящиеся к этому компьютеру.

Табл. 1-2 Symantec System Center

Значок	Описание значка
	Компьютер Windows 3.1. Устаревший клиент Symantec AntiVirus, работающий на компьютере под управлением Windows 3.1. При выполнении сплошной проверки в группе серверов, включающей таких клиентов, устаревшие клиенты также будут включены в осмотр. С консоли Symantec System Center такие компьютеры можно настраивать только на уровне группы серверов.
	На компьютере, на котором работает клиент Symantec AntiVirus Corporate Edition, обнаружен вирус.
	Клиент, на котором возникли неполадки, требующие устранения. Например, на клиенте могут быть обнаружены устаревшие файлы описаний вирусов, либо группа клиентов, к которой относится данный клиент, стала недопустимой. Информация об обнаруженной неполадке отображается в поле состояния консоли Symantec System Center.

Поиск компьютеров и обновление сведений на консоли

При первом запуске установленной консоли Symantec System Center консоль опрашивает сеть для поиска всех доступных компьютеров, на которых запущены серверы Symantec AntiVirus Corporate Edition. По мере получения ответов серверы добавляются в список консоли. Подключенные рабочие станции, на которых применяются управляемые клиентские продукты Symantec, добавляются, когда в иерархии консоли выбирается их *родительский сервер*.

Если серверы с управляемыми продуктами Symantec запускаются после запуска Symantec System Center, то для их отображения в окне просмотра группы серверов может потребоваться вызов функции «Найти компьютер» или службы обнаружения.

Применение службы обнаружения

Консоль Symantec System Center запускает одну службу Windows NT, – Symantec System Center Discovery Service (Nsctop.exe). Эта служба обеспечивает обнаружение компьютеров, на которых запущены серверы Symantec AntiVirus Corporate Edition, для отображения списка этих серверов в окне консоли Symantec System Center. Служба обнаружения также добавляет объекты в список консоли Symantec System Center.

Вы можете выбрать один из следующих типов обнаружения:

- Загружать только из кэша
- Локальное обнаружение
- Интенсивное обнаружение

См. «Информация об обнаружении с помощью загрузки из кэша» на стр. 20.

См. «Информация о локальном обнаружении» на стр. 20.

См. «Информация об интенсивном обнаружении» на стр. 21.

Обнаружение компьютеров в сети

Для обнаружения компьютеров в сети с компьютера, на котором работает сервер Symantec AntiVirus Corporate Edition, отправляется на компьютер, на котором работает клиент Symantec AntiVirus Corporate Edition, отправляется тестовый пакет. Тестовый пакет позволяет убедиться, что удаленный компьютер существует и может принимать запросы. Когда служба Intel Ping Discovery Service (Intel PDS) получает тестовый пакет, (ping), она передает соответствующий ответный пакет (pong). Пакеты запроса и ответа имеют размер около 1 Кб. Успешное обнаружение компьютера свидетельствует о работоспособности этого компьютера.

В ответном пакете (pong) передается различная информация, включая следующие сведения:

- Дата обновления файлов описаний вирусов на компьютере
- Дата последнего заражения компьютера

Для определения протоколов, поддерживаемых удаленным компьютером, на котором работает сервер Symantec AntiVirus Corporate Edition, этому компьютеру отправляются тестовые пакеты IP и IPX.

Кроме того, отправляются тестовые пакеты, поддерживающие устаревшие версии Symantec AntiVirus Corporate Edition: Norton AntiVirus Corporate Edition и LANDesk Virus Protect.

Данные с компьютера клиента Symantec AntiVirus Corporate Edition сохраняются на компьютере родительского сервера Symantec AntiVirus Corporate Edition, которому подчинен этот клиент.

Консоль Symantec System Center считывает из реестра всех родительских серверов данные и отображает их.

После завершения описанной процедуры запускается обычная процедура обнаружения.

Обычная процедура обнаружения

После выполнения всех перечисленных обнаружения запускается обычная процедура обнаружения. При обычном обнаружении консоль Symantec System Center передает широковещательные сообщения всем серверам, входящим в незаблокированные группы серверов. В ответ на эти дополнительные запросы первичный сервер группы серверов передает хранящийся в его адресном кэше список вторичных серверов.

В адресном кэше консоли Symantec System Center сохраняется информация, полученная когда-либо от любых серверов. Кэш адресов первичных серверов содержит сведения о всех серверах, входящих в группу серверов. В адресном кэше сохраняются имена и адреса IP всех вторичных серверов.

Консоль Symantec System Center сравнивает содержимое собственного адресного кэша с данными, полученными от первичного сервера. При обнаружении несоответствий консоль отправляет серверу тестовый пакет ping. После получения ответного пакета pong содержащиеся в нем данные добавляются на все серверы списка.

Таким образом обычная процедура обнаружения позволяет идентифицировать все серверы в группе серверов и пытается разрешить конфликты информации между родительскими серверами.

Требования службы обнаружения к WINS

Для работы службы обнаружения требуется наличие службы преобразования имен WINS (Windows Internet Naming Service). Если вы попытаетесь выполнить обнаружение в среде, не поддерживающей WINS, например, в стандартной сети Windows 2000, то сначала вам потребуется найти сначала хотя бы один подключенный к сети компьютер, на котором работает сервер Symantec AntiVirus Corporate Edition. Для этого можно воспользоваться функцией поиска компьютера или средством Importer.

См. «Применение функции поиска компьютера» на стр. 25.

Дополнительная информация о средстве Importer приведена в книге «*Symantec AntiVirus Corporate Edition: Справочник*».

Поиск компьютеров NetWare

Служба обнаружения не всегда обнаруживает компьютеры NetWare, использующие только протокол IP. Для поиска компьютеров, не найденных службой обнаружения, можно воспользоваться функцией «Найти компьютер».

См. «Применение функции поиска компьютера» на стр. 25.

Информация о настройке цикла обнаружения

Существует возможность настроить тайм-аут цикла обнаружения. В зависимости от того, как настроена служба обнаружения, можно задать интервал между попытками обнаружения от 1 до 1440 минут. По умолчанию установлен интервал в 480 минут (8 часов).

Если предыдущая попытка обнаружения не закончена, то новая попытка не предпринимается. Например, если обнаружение проводится один раз в минуту, а для завершения процесса необходимо 20 минут, то будет пропущено 19 попыток обнаружения.

Изменение интервала между циклами обнаружения

Интервал между циклами обнаружения можно изменить, но при этом следует учитывать, что увеличение этого интервала может привести к отображению устаревших сведений в консоли Symantec System Center.

Изменение интервала между циклами обнаружения

1 В меню «Сервис» консоли Symantec System Center выберите команду **Служба обнаружения**.

2 Установите новое значение параметра **Интервал (в минутах)**.

Информация об обнаружении с помощью загрузки из кэша

Этот способ является самым базовым способом обнаружения. Он пытается обновить информацию обо всех серверах, для которых есть записи в адресном кэше консоли Symantec System Center. Каждому серверу отправляется набор тестовых пакетов (ping) для проверки связи и на основании полученных ответов обновляется показанная на консоли информация.

После загрузки из кэша выполняется обычная процедура обнаружения.

См. «Обычная процедура обнаружения» на стр. 19.

Способ «Только загрузка из кэша» является способом обнаружения по умолчанию. Применение этого способа позволяет сократить сетевой трафик при запуске Symantec System Center. В большинстве случаев способ «Только загрузка из кэша» позволяет найти все серверы, которые необходимо добавить в список консоли Symantec System Center.

Информация о локальном обнаружении

При использовании локального обнаружения в локальную подсеть компьютера, на котором запущена консоль Symantec System Center,

отправляется широковещательный тестовый пакет. Службы Intel PDS, работающие на серверах локальной подсети, посылают ответные пакеты.

При локальном обнаружении создается небольшое количество запросов, но этот метод работает только в пределах локальной подсети. Метод локального обнаружения очень хорошо работает в небольших подсетях. В очень больших подсетях более эффективным оказывается метод интенсивного обнаружения.

После локального обнаружения могут применяться следующие способы обнаружения:

- Только загрузка из кэша
- Обычная процедура обнаружения

См. «Обычная процедура обнаружения» на стр. 19.

Информация об интенсивном обнаружении

Служба интенсивного обнаружения обращается к компоненту «Мое сетевое окружение» Windows 2000 или Windows NT на локальном компьютере и пытается определить сетевые адреса для всех найденных компьютеров. После получения сетевого адреса предпринимается попытка отправки тестового запроса (ping). Можно настроить интенсивное обнаружение для проверки ветви NetWare, ветви Microsoft, либо обеих ветвей структуры сети.

Для запуска новой процедуры обнаружения серверов можно выделить на консоли Symantec System Center один из объектов корневого каталога консоли, а затем выбрать команду «Служба обнаружения» в меню «Сервис».

После интенсивного обнаружения могут применяться следующие способы обнаружения:

- Локальное обнаружение
- Только загрузка из кэша
- Обычная процедура обнаружения

См. «Обычная процедура обнаружения» на стр. 19.

Примечание: Возможности интенсивного обнаружения по поиску компьютеров ограничены несколькими факторами: наличием сервера WINS, а также конфигурацией подсети, маршрутизатора, DNS, домена Microsoft и рабочей группы. На поиск по адресам IP эти ограничения в большинстве случаев не влияют. По этой причине в ряде случаев применяется обнаружение IP.

Информация об обнаружении IP

Обнаружение IP позволяет проводить обнаружение по диапазону адресов или по диапазону подсетей IP.

Возможно, вы сочтете целесообразным выполнять обнаружение IP лишь периодически. Эту функцию можно использовать для поиска компьютеров в сети.

После загрузки сведений о компьютерах в адресный кэш можно полностью перейти к способу «Только загрузка из кэша».

Запуск службы обнаружения

Все виды обнаружения запускаются вручную с консоли Symantec System Center.

Примечание: Служба обнаружения использует распознавание WINS (Windows Internet Name Service) для поиска новых компьютеров, на которых работает Symantec AntiVirus Corporate Edition. Если предпринимается попытка обнаружить новые компьютеры в среде, где распознавание WINS недоступно, например в сети Windows 2000, то целесообразно сначала запустить функцию «Найти компьютер» или программу Importer. См. «Применение функции поиска компьютера» на стр. 25. Дополнительная информация о средстве Importer приведена в книге «*Symantec AntiVirus Corporate Edition: Справочник*».

Запуск службы обнаружения

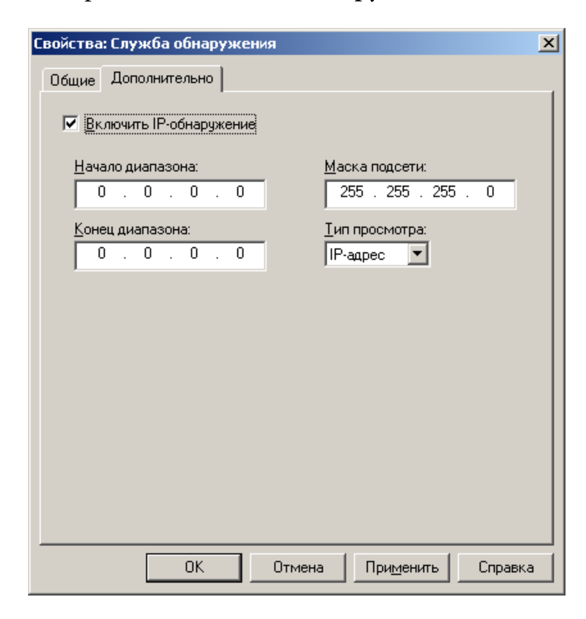
Запустить службу обнаружения для поиска серверов можно как с включением адресов IP и подсетей, так и без их включения.

Запуск обнаружения IP

1. На консоли Symantec System Center выберите в левой части окна любой узел, расположенный на верхнем уровне списка консоли.

2 В меню «Сервис» выберите команду **Служба обнаружения.**

3 В окне «Свойства службы обнаружения» на вкладке «Дополнительно» выберите **Включить IP-обнаружение.**



Если установлен флажок «Включить IP-обнаружение», то при запуске интенсивного обнаружения запускается сеанс обнаружения IP. Чтобы запустить интенсивное обнаружение, не запуская при этом обнаружение IP, снимите флажок «Включить IP-обнаружение».

4 В списке «Тип осмотра» выберите одно из следующих значений:

- Подсеть IP: Консоль рассылает широковещательные запросы в каждую подсеть
- Адрес IP: Консоль отправляет тестовый запрос ping всем компьютерам, адреса IP которых лежат в заданном диапазоне

5 В полях «Начало диапазона» и «Конец диапазона» укажите адреса.

6 Если выбран тип осмотра «Подсеть IP», введите маску подсети, чтобы ограничить область поиска.

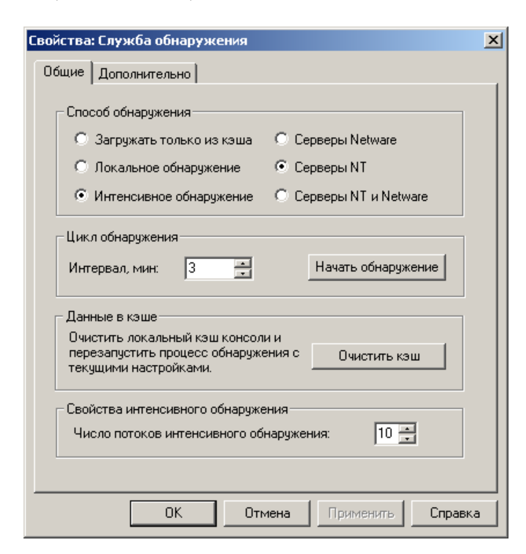
Результаты поиска по адресам IP появятся в списке «Компьютер». Результаты поиска в подсети IP отображаются в строке состояния консоли Symantec System Center.

Функция обнаружения IP также доступна через окно «Найти компьютер».

См. «Применение функции поиска компьютера» на стр. 25.

Обнаружение без применения IP

1 В меню «Сервис» консоли Symantec System Center выберите команду **Служба обнаружения.**



2 В окне свойств службы обнаружения на вкладке «Общие» выберите одно из следующих значений:

- Загружать только из кэша: Это самый быстрый способ. Symantec System Center считывает список серверов и клиентов, хранящийся в локальном кэше.

  См. «Информация об обнаружении с помощью загрузки из кэша» на стр. 20.

- Локальное обнаружение: В локальную подсеть консоли Symantec System Center отправляется широковещательный запрос. Серверы сразу отвечают и предоставляют данные о себе и своих клиентах. В списке консоли будут показаны все группы серверов (если в меню «Вид» не включен фильтр). Также может быть выполнено обнаружение «Загрузка только из кэша».

  См. «Информация о локальном обнаружении» на стр. 20.

- Интенсивное обнаружение: Это наиболее тщательный метод. В большой сети процесс обнаружения может занять достаточно длительное время. Symantec System Center последовательно опрашивает каждый сервер, представленный в окне «Сетевое окружение». Имена серверов появляются в строке состояния консоли Symantec System Center по мере их обнаружения. Кроме того, при интенсивном обнаружении по локальной подсети

отправляется такой же широковещательный запрос, как и при локальном обнаружении. Также может быть выполнено обнаружение «Загрузка только из кэша» и «Локальное обнаружение».

При интенсивном обнаружении можно ограничить область поиска только серверами NetWare или Windows NT, а можно искать серверы обоих типов.

См. «Информация об интенсивном обнаружении» на стр. 21.

3 При необходимости задайте интервал в минутах в разделе настройки цикла обнаружения.

4 Чтобы запустить обнаружение немедленно, выберите вариант **Начать обнаружение**, а затем нажмите кнопку **Закрыть**.

Одновременно может выполняться только одно обнаружение.

5 В окне свойств интенсивного обнаружения укажите число потоков интенсивного обнаружения.

Этот параметр влияет только на сеансы интенсивного обнаружения. Каждый поток обнаружения проводит независимый поиск серверов и клиентов. Чтобы получать наиболее актуальную информацию от службы обнаружения, выберите меньший интервал между сеансами и увеличьте число потоков обнаружения.

6 Чтобы сбросить все хранящиеся в активной памяти и локальном кэше данные обо всех серверах и клиентах и немедленно запустить сеанс обнаружения с текущими параметрами, нажмите кнопку **Очистить кэш**.

Если пароли групп серверов не запоминаются, то при очистке кэша будут заблокированы разблокированные группы серверов.

Примечание: Создание нового списка серверов для большой сети может занять длительное время.

Применение функции поиска компьютера

Для того чтобы быстро найти сервер, не выбирая объект в структуре системы, можно найти функцией поиска компьютера. Поиск можно выполнять по адресам TCP/IP или IPX, а также по именам компьютеров.

Функция «Найти компьютер» полезна также в том случае, если после установки сервера он не показывается в структуре системы при открытии группы серверов. Это может произойти по следующим причинам:

- Symantec System Center не может автоматически обнаружить серверы в сегментах локальной сети, разделенных маршрутизаторами.
- Серверы не показаны в окне «Сетевое окружение». Например, репликация серверов WINS (Windows Internal Naming Service) с пересечением границ сегмента сети не выполняется.

Серверы, находящиеся в сегментах, использующих только протокол IPX, также могут быть не найдены в процессе обнаружения. Если не удается найти некоторые серверы в локальной сети, то их можно попытаться найти с помощью функции поиска компьютера программы Symantec System Center. Обнаружив компьютер с помощью функции поиска, вы получаете возможность управлять им с помощью консоли Symantec System Center.

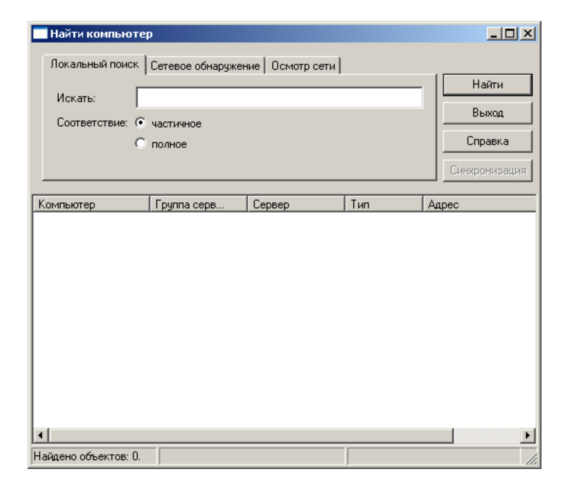
Примечание: Если протокол IPX не установлен, то вы не сможете увидеть с помощью консоли компьютеры NetWare. Эти компьютеры можно будет найти с помощью функции поиска компьютера, а после установки протоколов IPX и TCP/IP они будут обнаруживаться и службой обнаружения.

Поиск компьютеров в локальном кэше

Вместо того чтобы выполнять поиск компьютеров во всей сети, вы можете ограничиться поиском тех компьютеров, информация о которых точно присутствует в локальном кэше.

Поиск компьютеров в локальном кэше

1. В меню «Сервис» консоли Symantec System Center выберите команду **Найти компьютер**.



2. В окне «Найти компьютер» на вкладке «Локальный поиск» введите сетевое имя сервера, который нужно найти.
3. В группе параметров «Тип соответствия» выберите один из следующих вариантов:
   - Полное: Выполняет поиск имени сервера, точно совпадающего с указанным
   - Частичное: Выполняет поиск имени сервера, частично совпадающего с указанным

   Если оставить поле «Искать» пустым и использовать частичное соответствие, то в списке результатов поиска появятся все компьютеры из локального кэша.

Поиск компьютеров в сети

Сетевой поиск позволяет найти отдельные компьютеры, на которых применяется сервер Symantec AntiVirus Corporate Edition.

Поиск компьютеров

Для поиска компьютеров можно воспользоваться функцией сетевого поиска, задать адрес IP или диапазон подсети.

Поиск компьютеров в сети

1. В меню «Сервис» консоли Symantec System Center выберите команду **Найти компьютер**.
2. В окне поиска компьютера на вкладке «Сетевое обнаружение» укажите, какие данные будут применяться в качестве условия поиска: адрес TCP/IP, адрес IPX или имя компьютера.
3. Введите адрес или имя компьютера.
4. Нажмите кнопку **Найти**.

Поиск компьютеров с работающим сервером Symantec AntiVirus Corporate Edition по диапазону адресов IP

1. В меню «Сервис» консоли Symantec System Center выберите команду **Найти компьютер**.
2. В окне поиска компьютеров на вкладке «Осмотр сети» выберите одно из следующих значений:
   - Подсеть IP: Рассылает широковещательные пакеты во все подсети
   - Адрес IP: Отправляет тестовый запрос ping всем компьютерам, адреса IP которых лежат в заданном диапазоне
3. Введите адреса начала диапазона и конца диапазона.
4. Если на этапе 2 выбран тип осмотра «Подсеть IP», введите маску подсети, чтобы ограничить область поиска.
5. Нажмите кнопку **Найти**.

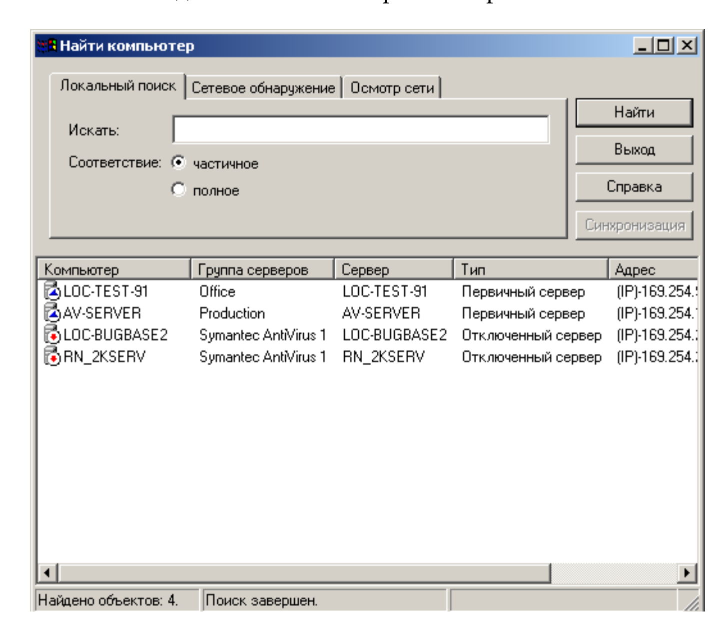
   Результаты поиска по адресам IP появятся в списке «Компьютер». Результаты поиска в подсети IP будут отображаться в строке состояния консоли Symantec System Center.

Выделение найденных объектов в консоли Symantec System Center

Для каждого объекта, представленного в списке найденных компьютеров, можно найти и выделить соответствующий объект в структуре списка консоли Symantec System Center. Для этого группа серверов, к которой принадлежит искомый объект, должна быть разблокирована.

Выделение найденных объектов в консоли Symantec System Center

1 В списке найденных компьютеров выберите объект.



2 Для поиска выбранного объекта нажмите кнопку **Синхронизация.**

Применение функции обновления

Консоль Symantec System Center позволяет обновлять сведения на уровне структуры системы, группы серверов или отдельного сервера, чтобы проверить доступность представленных в текущем списке серверов. Однако при обновлении сведений не производится поиск отдельных серверов или групп серверов, которые могли быть добавлены с начала текущего сеанса работы с Symantec System Center. Если при обновлении сведений обнаружится, что какой-либо из серверов группы не отвечает на запросы, появится значок недоступного сервера.

Применение функции обновления

◆ В консоли Symantec System Center щелкните правой кнопкой мыши на объекте структуры системы, разблокированной группе серверов или на сервере, и выберите команду **Обновить**.

Сведения о клиентах и серверах

Клиент Symantec AntiVirus Corporate Edition обеспечивает антивирусную защиту как автономных компьютеров, так и компьютеров, подключенных к сети. Клиент Symantec AntiVirus Corporate Edition может защищать компьютеры, работающие под управлением Windows 98/Me/NT/2000/XP.

Для защиты компьютеров, работающих под управлением Windows 95/3.1/DOS, применяется клиент Norton AntiVirus Corporate Edition 7.6.

Сервер Symantec AntiVirus Corporate Edition обеспечивает управление другими компьютерами, на которых применяется Symantec AntiVirus Corporate Edition, и может передавать клиентам Symantec AntiVirus Corporate Edition данные конфигурации и обновленные файлы описаний вирусов. Кроме того, программное обеспечение Symantec AntiVirus Corporate Edition обеспечивает антивирусную защиту компьютеров, на которых оно установлено. Клиенты Symantec AntiVirus Corporate Edition всегда находятся под управлением серверов.

С точки зрения управления программой Symantec System Center, компьютеры, на которых работают серверы Symantec AntiVirus Corporate Edition, могут выступать в следующих ролях:

- Первичный сервер
- Вторичный сервер
- Родительский сервер

Сведения о первичных серверах

В каждой группе серверов имеется назначенный администратором *первичный сервер*. Первичный сервер отвечает за настройку всех входящих в группу компьютеров. Он также может быть ответственным за обновление файлов вирусных описаний.

Если с помощью консоли Symantec System Center запустить какую-либо задачу на уровне группы серверов, эта задача выполняется на первичном сервере группы. Кроме того, первичный сервер передает эту задачу всем остальным серверам, входящим в группу.

Если используется Alert Management System[2], то первичный сервер берет на себя обработку уведомлений.

Первичным сервером можно сделать компьютер, работающий под управлением одной из перечисленных ниже операционных систем.

- Windows 2000 Server, Advanced Server или Professional
- Windows NT 4.0 Server или Workstation
- NetWare 3.x, 4.x, 5.x или 6

Как изменяется реестр

При изменении параметров серверов внесенные изменения вносятся непосредственно в реестры выбранных серверов. Изменения вносятся посредством транспортного уровня, обеспечивающего связь.

Первичный сервер является хранилищем всех параметров серверов на уровне группы. Все изменения, вносимые на уровне группы, записываются в реестр на первичном сервере этой группы в ключ

HKEY_LOCAL_MACHINE\SOFTWARE\INTEL\LANDesk\VirusProtect6\DomainData

Затем они записываются на все остальные серверы.

Сведения о вторичных серверах

Серверы, которые не были выбраны в качестве первичных серверов, называются *вторичными серверами*. Вторичные серверы являются дочерними по отношению к первичным серверам. Они получают информацию с первичного сервера и используют ее совместно со своими клиентами.

Все серверы, входящие в группу, являются вторичными серверами до тех пор, пока один из них не будет выбран в качестве первичного сервера. Чтобы получить возможность выполнения большинства операций на уровне группы, необходимо назначить один из серверов первичным сервером.

Примечание: Изменением конфигурации продуктов Symantec нельзя управлять на более высоком уровне, чем уровень группы серверов.

Сведения о родительских серверах

Родительский сервер представляет собой компьютер, на котором работает сервер Symantec AntiVirus Corporate Edition, и которой взаимодействует с компьютером клиента Symantec AntiVirus Corporate Edition, передавая

клиенту обновленные параметры конфигурации и обрабатывая полученные от клиента предупреждения. Одни серверы могут выступать в качестве родительских серверов, другие могут быть первичными серверами. Эти две роли не являются взаимоисключающими. Первичный сервер может выступать и в роли родительского сервера.

Сведения о группах клиентов и серверов

Компьютеры, входящие в *группу серверов*, могут применять общую конфигурацию Symantec AntiVirus Corporate Edition; кроме того, можно выполнять операции Symantec AntiVirus Corporate Edition над всеми компьютерами, входящими в группу серверов. С помощью консоли Symantec System Center можно создавать новые группы серверов и управлять их элементами. Группы серверов не зависят от доменов Windows NT/2000 и других продуктов. В одну группу можно включить и серверы NetWare, и серверы Windows NT, и серверы Windows 2000, что дает возможность одновременной дистанционной настройки этих систем.

Группы клиентов представляют собой логические группы, объединяющие компьютеры, на которых работает программное обеспечение клиента Symantec AntiVirus Corporate Edition. Несмотря на то, что группы клиентов всегда связаны с группой сервера, каждой группой клиентов можно управлять независимо. Настроив несколько групп клиентов для одного родительского сервера, вы можете создавать и применять к этим группам различные политики управления.

- *Присвоенные клиенты* — это клиенты Symantec, входящие в какую-либо группу клиентов. Описания вирусов такие клиенты могут получать с сервера, к которому они подключены физически, однако их обновление и изменение параметров настройки определяются группой клиентов, к которой применяются политики Symantec AntiVirus Corporate Edition.
- *Не присвоенные клиенты* — это клиенты Symantec, которые не входят ни в одну группу клиентов. Такие клиенты получают параметры настройки и обновления со своего родительского сервера.

Выбор между управлением с помощью групп клиентов и серверов

В каждой группе серверов Symantec AntiVirus Corporate Edition для всех управляемых клиентов поддерживается одна общая конфигурация. Создание дополнительных конфигураций требует добавления новых серверов в группу. Если на всех клиентах должна применяться одинаковые

параметры конфигурации, то группы серверов оказываются достаточно эффективным решением. Если же необходима большая гибкость настройки, то можно воспользоваться группами клиентов. При управлении с помощью групп клиентов подключенные к одному физическому серверу клиенты могут применять разные конфигурации. Кроме того, группы клиентов позволяют сократить число серверов, необходимых для управления Symantec AntiVirus Corporate Edition. Если в группе серверов для каждой конфигурации необходим по крайней мере один сервер, то число групп клиентов в группе серверов может быть любым, а каждой группе клиентов может соответствовать собственная конфигурация.

Примечание: При использовании групп клиентов Symantec рекомендует организовать управление всеми клиентами с помощью групп. Несмотря на то, что в принципе можно управлять средой, в которой некоторые клиенты включены в группы, а некоторые нет, такое управление оказывается достаточно сложным и может привести к непредсказуемым результатам.

Группы клиентов и приоритет настройки

Если для управления применяются группы клиентов, то все входящие в группы клиенты получают параметры настройки из своей группы, а не от родительского сервера. Изменение параметров настройки, вносимое на уровне сервера, игнорируется и применяется только к клиентам, не входящим в группы. Изменения, вносимые на уровне группы сервера или на уровне структуры системы, имеют более высокий приоритет, чем параметры группы клиентов, поэтому они переопределяют все значения, заданные на уровне группы клиентов.

Табл. 1-3 содержит список контекстов Symantec System Center с указанием области объектов, к которой применяются параметры настройки, заданные при выборе каждого контекста.

Табл. 1-3 Приоритет настройки

Контекст	Настраиваемые объекты
Структура системы	Все разблокированные группы серверов и управляемые ими клиенты (независимо от их вхождения в группы клиентов)
Группа серверов	Все серверы и клиенты в группе серверов (независимо от их вхождения в группы клиентов)

Табл. 1-3 Приоритет настройки

Контекст	Настраиваемые объекты
Сервер	Сервер и его клиенты (независимо от их вхождения в группы клиентов): ■ Сплошные проверки ■ Обновление описаний вирусов ■ Настройка журнала Сервер и/или его не присвоенные клиенты: ■ Плановые осмотры и осмотры вручную ■ Обновление описаний вирусов ■ Параметры изолятора ■ Параметры постоянной защиты сервера и клиента ■ Параметры клиента (только для администратора) ■ Функция LiveUpdate ■ Состояние постоянной защиты файловой системы ■ Просмотр списка вирусов ■ Сброс данных о зараженном состоянии
Группы клиентов	Клиенты, входящие в группы клиентов: ■ Плановые осмотры ■ Обновление описаний вирусов ■ Параметры изолятора ■ Настройка журнала ■ Параметры постоянной защиты клиента ■ Параметры клиента (только для администратора) ■ Функция LiveUpdate
Клиент	Только чтение

Сценарий настройки групп клиентов и серверов

В организации есть отдел маркетинга и бухгалтерия. Персонал этих отделов работает в филиалах компании, расположенных в Москве, Санкт-Петербурге и Новосибирске. Все компьютеры обоих отделов входят в одну и ту же группу серверов, поэтому они получают обновления описаний вирусов из одного источника. Однако исследования, проведенные отделом информационных технологий, показывают, что отдел маркетинга более подвержен заражению вирусами, чем бухгалтерия. В результате системный администратор принял решение о создании отдельных групп клиентов для бухгалтерии и для отдела маркетинга. Теперь клиентские компьютеры

отдела маркетинга применяют общие параметры настройки, весьма строго регламентирующие взаимодействие пользователей со средствами антивирусной защиты.

Управление с помощью групп серверов

Вы можете создать столько групп серверов, сколько необходимо для эффективного управления всеми имеющимися серверами и клиентами.

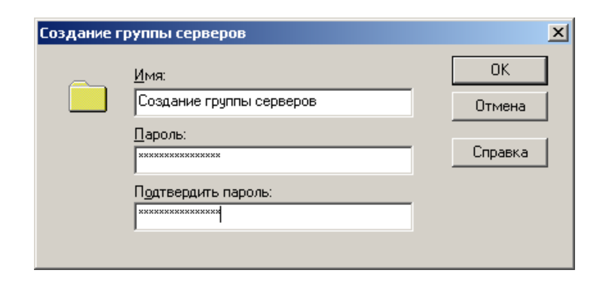
Создание групп серверов

Программа установки объединяет все серверы, выбранные для установки программного обеспечения, в одну группу серверов. Такой подход правилен в том случае, если на всех компьютерах, применяющих Symantec AntiVirus Corporate Edition, должны быть заданы одинаковые параметры настройки. Однако для внесения глобальных изменений в конфигурацию групп серверов можно создать новые группы и с помощью мыши (или с помощью команд копирования и вставки) быстро перенести в эти группы требуемые серверы. Вместе с сервером перемещаются и все подключенные к нему клиенты.

Например, если в сети есть серверы, требующие максимальной защиты, то вы можете поместить их в одну группу серверов и задать для этой группы особые параметры защиты. (Обратите внимание, что для достижения той же цели можно создать и новую группу клиентов. См. раздел «Сведения о группах клиентов и серверов» на стр. 32.

Создание группы серверов

1 В консоли Symantec System Center щелкните правой кнопкой мыши на компоненте **Структура системы** и выберите команду **Создать** > **Группа серверов**.



2 В окне создания группы серверов введите имя группы.

Длина имени не должна превышать 47 знаков.

3 В поле пароля введите пароль доступа к группе.

4 В поле подтверждения пароля введите пароль еще раз.

5 Нажмите кнопку **OK**.

В каждой группе серверов должен быть первичный сервер.

См. «Выбор первичного сервера группы» на стр. 39.

Блокировка и разблокирование групп серверов

Вы можете защитить группу паролем для предотвращения несанкционированного доступа и изменения конфигурации администраторами, не имеющими соответствующих полномочий. Установить защиту или изменить пароль можно в любое время. По умолчанию для групп серверов, создаваемых при установке, задается следующий пароль:

symantec

Пароли вводятся с учетом регистра.

Блокировка и разблокирование групп серверов

Вы можете блокировать и разблокировать группы серверов по мере необходимости. Для разблокирования группы необходимо правильно ввести пароль. Пароли вводятся с учетом регистра. Кроме того, можно запретить блокировку групп серверов при завершении работы с консолью.

Блокировка группы серверов

◆ В консоли Symantec System Center щелкните правой кнопкой мыши в левой части окна на группе серверов, которую необходимо блокировать, и выберите **Заблокировать группу**.

Разблокирование группы серверов

1 В консоли Symantec System Center щелкните правой кнопкой мыши в левой части окна на группе, которую необходимо разблокировать, и выберите команду **Разблокировать группу**.

2 Введите пароль для разблокирования группы.

3 Установите флажок **Сохранить пароль**, чтобы не вводить пароль повторно в следующих сеансах или для других групп серверов, защищенных таким же паролем.

Если пароль введен правильно, он будет сохранен.

Запрет блокировки групп серверов при завершении работы с консолью

1. В консоли Symantec System Center щелкните правой кнопкой мыши на компоненте структуры системы и выберите команду **Свойства**.
2. Снимите флажок **Блокировать все группы при выходе из консоли**.

Работа с паролями групп серверов

По мере необходимости вы можете сохранять и изменять пароли групп серверов, а также удалять сохраненные пароли. Для выполнения этих операций в группе серверов должен быть выделен родительский сервер. Разрешаются пустые пароли.

Сохранение пароля группы серверов

Вы можете сохранить пароли, чтобы избежать их повторного ввода в последующих сеансах. Если пароль сохранен, то его не требуется вводить при открытии любой группы серверов, защищенной таким же паролем. Сохраненные пароли шифруются с помощью алгоритма DES и сохраняются в реестре локального компьютера. При попытке разблокировать какую-либо группу серверов Symantec System Center применит все сохраненные пароли. Ввести пароль потребуется только в том случае, если ни один из сохраненных паролей не подойдет.

Сохранение паролей групп серверов и удаление сохраненных паролей

Флажок «Сохранить пароль» позволяет сохранить введенный пароль, чтобы не вводить его при следующем открытии группы серверов.

Если пароль сохранен, то все группы серверов, к которым вы обращались, будут либо разблокированы, либо не будут запрашивать у вас пароль при попытке снятия блокировки.

Если на странице свойств структуры системы снят флажок «Блокировать все группы при выходе из консоли», то при повторном открытии консоли Symantec System Center группы серверов останутся разблокированными.

Если пароли не запоминаются, то все группы серверов автоматически блокируются при каждом запуске Symantec System Center, даже если они были разблокированы во время последнего сеанса работы с программой.

Сохранение пароля группы серверов

1. В консоли Symantec System Center щелкните правой кнопкой мыши в левой части окна на блокированной группе серверов и выберите команду **Разблокировать группу**.
2. Введите пароль группы серверов.

   Если пароль сервера уже был задан и вы отметили флажок **Сохранить пароль**, то окно ввода пароля не появится. Задайте новый пароль, который будет применяться данной функцией.
3. Установите флажок **Сохранить пароль**.
4. Нажмите кнопку **OK**.

См. «Изменение пароля группы серверов» на стр. 38.

Удаление сохраненного ранее пароля группы серверов

1. В консоли Symantec System Center щелкните правой кнопкой мыши в левой части окна на разблокированной группе серверов и выберите команду **Блокировать группу**.
2. Введите старый пароль.
3. Нажмите клавишу **Tab** и введите новый пароль.
4. Еще раз нажмите клавишу **Tab** и введите новый пароль еще раз.
5. Нажмите кнопку **OK**.
6. Закройте консоль Symantec System Center.
7. Если вам будет предложено сохранить пароль, ответьте **Нет**.

Изменение пароля группы серверов

Вы можете изменять пароли групп серверов. Например, можно изменять пароли регулярно для обеспечения более надежной защиты.

Изменение пароля группы серверов

1. В консоли Symantec System Center щелкните правой кнопкой мыши на группе серверов и выберите **Настроить пароль группы серверов**.
2. Введите старый пароль.
3. Нажмите клавишу **Tab** и введите новый пароль.
4. Еще раз нажмите клавишу **Tab** и введите новый пароль еще раз.
5. Нажмите кнопку **OK**.

Переименование групп серверов

Вы можете переименовывать группы серверов.

Переименование группы серверов

1 При необходимости разблокируйте с помощью консоли Symantec System Center группу серверов, которую нужно переименовать.

2 Щелкните правой кнопкой мыши на группе серверов и выберите команду **Переименовать**.

3 Введите новое имя группы серверов.

Выбор первичного сервера группы

Когда в программе Symantec System Center выбирается группа серверов и настраиваются ее параметры, эти параметры сохраняются на первичном сервере группы. Другие серверы, входящие в группу, будут использовать сохраненную новую конфигурацию.

Необходимо указать, какой сервер в группе является первичным. По умолчанию первичный сервер не задается. Пока не будет задан первичный сервер, вы не сможете выполнять некоторые операции управления программными продуктами Symantec.

Первичным сервером может быть компьютер, работающий под управлением одной из следующих операционных систем.

- Windows 2000 Server, Advanced Server или Professional
- Windows XP Professional
- Windows NT 4.0 Server или Workstation
- NetWare Server

Первичный сервер имеет большое значение, поэтому в качестве первичного следует выбирать постоянно включенный стабильный сервер.

Выбор первичного сервера группы

◆ В консоли Symantec System Center щелкните правой кнопкой мыши в левой части окна на сервере, которой необходимо сделать первичным сервером группы, и выберите **Сделать сервер первичным**.

Примечание: При изменении первичных серверов теряются настроенные предупреждения системы AMS[2]. Можно настроить предупреждения заново на новом первичном сервере, но предусмотрена и возможность экспорта настройки предупреждений на новый сервер перед сменой первичного сервера.

Изменение первичных и родительских серверов

Вы можете легко изменять выбор первичных и родительских серверов.

Изменение первичных серверов

При необходимости вы можете отменить выбор какого-либо сервера в качестве первичного и сделать первичным сервер, используемый в данный момент в качестве вторичного.

Изменение первичного сервера

1 В структуре объектов консоли Symantec System Center дважды щелкните на значке группы серверов.

2 Щелкните правой кнопкой на вторичном сервере, который следует сделать первичным, затем выберите команду **Сделать сервер первичным**.

Изменение родительских серверов клиентов

Для изменения родительского сервера необходимо скопировать на клиента файл конфигурации (Grc.dat) с нового родительского сервера, а затем перезапустить клиента.

Файл конфигурации представляет собой текстовый файл, в котором хранятся сведения об изменениях, вносимых в конфигурацию группы клиентов. Файлы конфигурации являются ключевым компонентом, обеспечивающим связь между компьютерами, на которых работает сервер Symantec AntiVirus Corporate Edition, и компьютерами, на которых запущены клиенты Symantec AntiVirus Corporate Edition. В них хранится важная информация, включая сведения о родительском сервере и параметры конфигурации продукта Symantec AntiVirus Corporate Edition.

Изменение родительского сервера для клиента

1 На сервере, который будет применяться в качестве нового родительского сервера, скопируйте файл конфигурации (Grc.dat) из каталога \Program Files\SAV\.

2 На клиентах файл конфигурации следует поместить в следующие каталоги:

- В системах Windows 98\Me: C:\Program Files\Norton AntiVirus
- В системах Windows NT: C:\Winnt\Profiles\All Users\Application Data\Symantec\Norton AntiVirus Corporate Edition\7.5
- В системах Windows 2000\XP: C:\Documents and Settings\All Users\Application Data\Symantec\Norton AntiVirus Corporate Edition\7.5

3 Перезапустите клиента.

Перемещение сервера в другую группу серверов

Перемещать серверы из одной группы в другую можно методом перетаскивания.

При перемещении сервера на нем автоматически создается файл конфигурации сервера (Grcsrv.dat). Этот файл позволяет синхронизовать параметры сервера с параметрами новой группы. В новой группе серверов должен быть задан первичный сервер.

Файл конфигурации сервера располагается в том же каталоге, в который на сервере устанавливается продукт Symantec AntiVirus Corporate Edition. Его формат совпадает с форматом файла конфигурации клиента (Grc.dat). Этот файл создается лишь при синхронизации параметров сервера с параметрами новой группы серверов.

Файл конфигурации сервера применяется только для серверов, на которых запущен Norton AntiVirus Corporate Edition 7.5 или более поздней версии, а также для серверов Symantec AntiVirus Corporate Edition. На серверах более старых версий служба топологии копирует параметры реестра с первичного сервера на перемещаемый сервер.

Просмотр групп серверов

С помощью консоли Symantec System Center можно просматривать серверы, на которых запущены управляемые программы Symantec AntiVirus Corporate Edition, в виде иерархической структуры. Серверы в этой структуре объединены в группы.

Просмотр отдельной группы серверов

Вы можете просмотреть отдельную группу серверов и ее содержимое.

Просмотр отдельной группы серверов

- В консоли Symantec System Center щелкните правой кнопкой мыши на нужной группе серверов и выберите команду **Создать новое окно**.

Фильтр для просмотра групп серверов

Имеется возможность использовать фильтр при просмотре групп серверов в списке Symantec System Center. Вы можете отслеживать и администрировать только те группы серверов, которые представлены в списке. По умолчанию в консоли Symantec System Center отображаются все группы серверов. Для того чтобы убрать из списка консоли отдельные группы серверов, следует включить фильтр просмотра.

Вы будете получать уведомления о событиях только для отображаемых групп серверов. Если группа серверов отфильтрована, то уведомления о событиях для этой группы вы получать не будете.

Включение фильтра для просмотра групп серверов

1. В консоли Symantec System Center щелкните правой кнопкой мыши на компоненте структуры системы и выберите команду **Вид** > **Фильтр для просмотра групп серверов**.
2. Снимите флажки для групп серверов, которые необходимо исключить из списка групп.

   По умолчанию отображаются все группы серверов.
3. Нажмите кнопку **OK**.

Удаление групп серверов

Перед удалением группы серверов необходимо перенести входящие серверы в другую группу.

Удаление группы серверов

1. В консоли Symantec System Center щелкните правой кнопкой мыши в левой части окна на группе серверов, которую необходимо удалить, и выберите команду **Удалить группу**.
2. Переместите все серверы из удаляемой группы в другую группу серверов методом перетаскивания.

Удалить можно только пустую группу серверов.

3 Щелкните правой кнопкой мыши на пустой группе серверов и выберите команду **Удалить**.

4 Щелкните правой кнопкой на компоненте структуры системы и выберите команду **Обновить**.

Управление с помощью групп клиентов

Вы можете создать столько групп, сколько необходимо для эффективного управления всеми имеющимися клиентами.

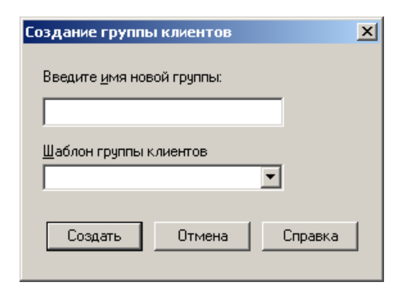
Создание новых групп клиентов

Во всех группах серверов есть отдельная папка «Группы», в которой перечислены все группы, связанные с данной группой серверов. При создании новой группы клиентов эта группа появляется в папке «Группы».

Создание новой группы клиентов

1 В консоли Symantec System Center щелкните правой кнопкой мыши в левой части окна на группе серверов, в которой необходимо создать группу клиентов, и выберите **Разблокировать группу**.

2 Щелкните правой кнопкой мыши на папке «Группы» и выберите команду **Создать группу**.



3 В окне создания новой группы укажите имя новой группы клиентов.

Длина имени не должна превышать 15 знаков.

4 Для применения к новой группе клиентов параметров уже существующей группы выберите в списке имя существующей группы.

5 Нажмите кнопку **Создать**.

Добавление клиентов в группу клиентов

В группы клиентов можно добавлять компьютеры, на которых применяется сервер Symantec AntiVirus Corporate Edition, клиент или устаревшие версии программного обеспечения. Все клиенты обрабатываются одинаково. Если на устаревшем клиенте Norton AntiVirus отсутствует функция, для которой задаются параметры настройки, то значения этих параметров игнорируются.

Примечание: Группы клиентов поддерживаются только серверами Symantec AntiVirus Corporate Edition. Они не поддерживаются устаревшими версиями Norton AntiVirus Corporate Edition.

Клиент может входить только в одну группу клиентов.

Добавление клиента в группу клиентов

1. В консоли Symantec System Center в левой части окна щелкните на сервере, к которому относится клиент.
2. В правой части окна перетащите клиента с помощью мыши в нужную группу клиентов.

Настройка параметров и выполнение задач на уровне группы клиентов

Вы можете задавать параметры конфигурации и различные выполнять задачи на уровне групп клиентов. Параметры будут применены ко всем клиентам группы, задачи также будут выполнены на всех входящих в группу клиентах.

Настройка параметров и выполнение задач на уровне группы клиентов

1. В консоли Symantec System Center щелкните правой кнопкой мыши на группе клиентов в левой части окна.
2. Выберите **Все задачи**.
3. Щелкните на продукте, для которого необходимо задать параметры.
4. Выберите тип настраиваемых параметров или задачу для выполнения.

Поиск параметров групп клиентов

Параметры групп клиентов хранятся в реестре первичного сервера. Они устанавливаются на каждый сервер в файле конфигурации клиента (Grcgrp.dat). Первичный сервер упаковывает все параметры групп клиентов в файл конфигурации группы, а затем копирует этот файл на все вторичные серверы, входящие в состав группы серверов. Вторичные серверы передают параметры своим управляемым клиентам.

Дополнительная информация о файлах конфигурации приведена в книге *«Symantec AntiVirus Corporate Edition: Справочник»*.

Перемещение клиентов между группами

Вы можете переносить клиентов из одной группы клиентов в другую методом перетаскивания. После перемещения клиент получает параметры конфигурации новой группы клиентов.

Просмотр групп клиентов

При просмотре групп клиентов вы можете выполнять следующие операции:

- Просмотр отдельной группы клиентов
- Просмотр информации о группах клиентов
- Фильтрация списка групп клиентов для просмотра только интересующей вас информации

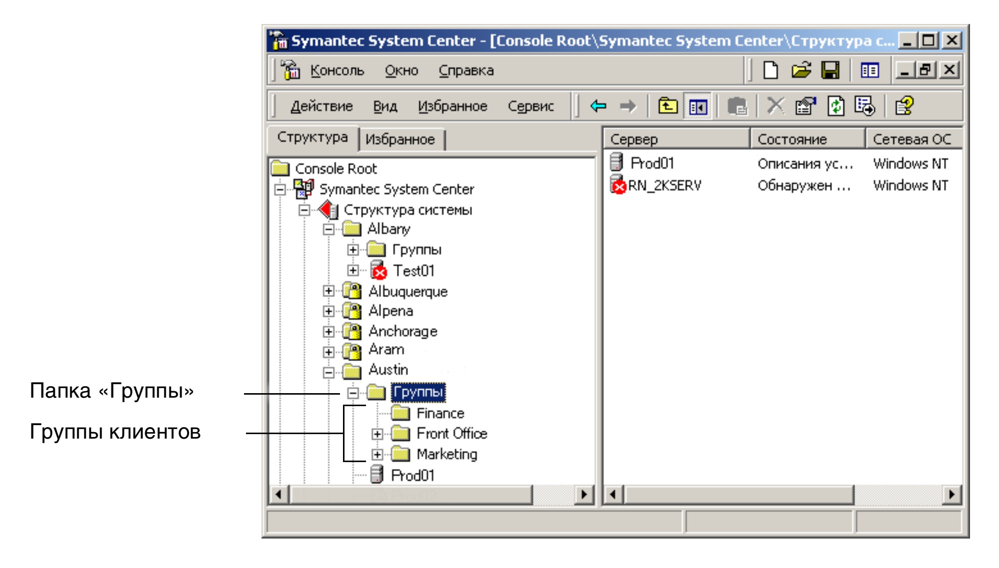
Просмотр отдельной группы клиентов

Вы можете просматривать содержимое отдельных групп клиентов.

Просмотр отдельной группы клиентов

1. В консоли Symantec System Center щелкните правой кнопкой мыши в левой части окна на группе серверов, в которую входит группа клиентов, и выберите команду **Разблокировать группу**.
2. Дважды щелкните на группе серверов.

3 Дважды щелкните на папке **Группы**.



Будут показаны группы клиентов, расположенные в папке «Группы».

Просмотр информации о группах клиентов

Если в левой части окна выбрана папка «Группы», а в меню «Вид» выбран режим просмотра консоли по умолчанию или режим просмотра продуктов Symantec, то в правой части окна будут перечислены группы клиентов, а также информация, применимая для выбранного режима. Например, при выборе режима просмотра консоли по умолчанию будут показаны сведения о числе клиентов в каждой группе клиентов.

Для просмотра списка клиентов необходимо включить фильтр групп клиентов. Число клиентов, показанное для группы после выбора папки «Группы», но до момента выбора группы клиентов, может быть неточным.

См. «Фильтр для просмотра групп клиентов» на стр. 46.

Фильтр для просмотра групп клиентов

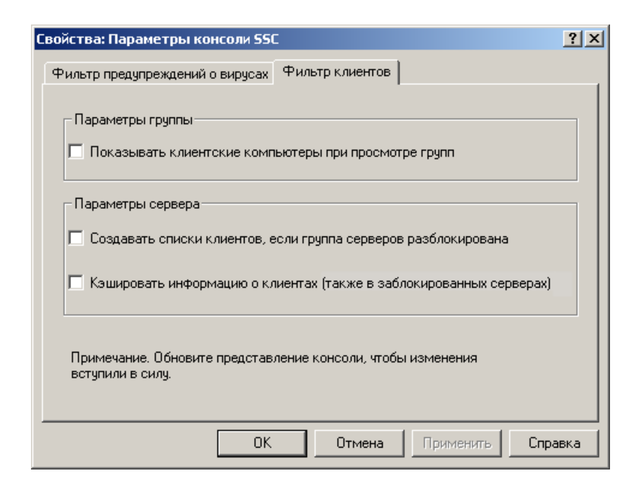
При выборе в левой части окна группы клиентов в правой части окна могут быть показаны все клиенты, входящие в эту группу.

Применение фильтра повышает отображения списков при просмотре клиентов в консоли Symantec System Center. Однако при наличии в группе серверов большого числа серверов и клиентов применение фильтра может привести к снижению производительности. Для правильного отображения

информации о группах клиентов необходим список клиентов. По умолчанию фильтр выключен.

Включение фильтра для просмотра групп клиентов

1 В меню «Сервис» консоли Symantec System Center выберите команду **Параметры консоли SSC**.



2 В окне свойств параметров консоли SSC на вкладке «Фильтр клиентов» в разделе «Параметры групп» выберите **Показывать клиентские компьютеры при просмотре групп**.

3 В разделе «Параметры серверов» выберите любые параметры из следующего списка:

- Создавать списки клиентов, если группа серверов разблокирована: Показывает всех клиентов в разблокированной группе сервера.

  Если этот параметр не выбран, то клиенты не добавляются в группу клиентов до тех пор, пока сервер не будет выбран. Показанное число клиентов в группе будет неправильным, пока не будут выбраны все серверы, входящие в группу серверов.
- Кэшировать информацию о клиентах (включая клиентов в заблокированных группах): Показывает клиентов в блокированных и разблокированных группах, обнаруженных службой топологии.

При большом числе клиентов и серверов в группе серверов выбор этих параметров может привести к снижению производительности.

4 Нажмите кнопку **OK**.

5 В меню «Действие» выберите **Обновить**.

Переименование групп клиентов

Symantec System Center не поддерживает непосредственное переименование групп клиентов. Для изменения имени группы клиентов необходимо выполнить следующие действия:

- Создать новую группу клиентов и при необходимости импортировать в нее параметры существующей группы.

  См. «Создание новых групп клиентов» на стр. 43.
- Методом перетаскивания переместить клиентов из старой группы клиентов в новую.
- Удалить старую группу клиентов.

  См. «Удаление групп клиентов» на стр. 48.

Удаление групп клиентов

Перед удалением группы клиентов рекомендуется присвоить клиентов другим группам клиентов.

При удалении группы клиентов на всех входивших в ее состав клиентах сохраняются параметры удаленной группы. Новые параметры не задаются для клиентов до наступления любого из следующих событий:

- Клиент устанавливает соединение со своим родительским сервером. После этого на клиенте устанавливаются параметры по умолчанию для не присвоенных клиентов.
- Клиент включается в другую группу клиентов. После этого на клиенте устанавливаются параметры новой группы клиентов.

Если вы удалите группу клиентов, а потом вновь создадите ее до того, как клиенты подключатся к своим родительским серверам или будут включены в другие группы, то членство клиентов в группе будет автоматически восстановлено. При этом на клиентах по-прежнему будут применяться параметры данной группы.

Удаление группы клиентов

1. В консоли Symantec System Center выберите в левой части окна группу серверов, из которой необходимо удалить группу клиентов, и разблокируйте эту группу серверов.
2. Дважды щелкните на группе серверов.
3. Дважды щелкните на папке **Группы**.

4 Щелкните правой кнопкой мыши на удаляемой группе и выберите команду **Удалить**.

5 Нажмите кнопку **Да**.

6 Нажмите кнопку **Удалить**.

Переключение между управляемым и автономным клиентом

Вы можете сделать автономного клиента управляемым и наоборот.

Изменение режима управления для клиента

После того, как вы сделаете автономного клиента управляемым клиентом, он будет показан в списке Symantec System Center и его можно будет настраивать с помощью Symantec System Center. Если же вы сделаете управляемого клиента автономным, то он будет удален из списка Symantec System Center.

Переключение автономного клиента в режим управляемого клиента

1. Решите, какой сервер будет выполнять функции родительского сервера для данного клиента.
2. Откройте папку «Сетевое окружение».
3. Найдите компьютер, который будет выполнять функции родительского сервера, и дважды щелкните на его имени.

   На выбранном компьютере должен быть установлен сервер Symantec AntiVirus Corporate Edition.
4. Откройте папку **VPHOME\Clt-inst\Win32**
5. Скопируйте файл Grc.dat в выбранную папку.
6. Поместите файл Grc.dat в следующую папку автономного клиента:
   - Windows 98/Me C:\Program Files\Norton AntiVirus
   - Windows NT 4.0: C:\Winnt\Profiles\All Users\Application Data\Symantec\Norton AntiVirus Corporate Edition\7.5
   - Windows 2000/XP: C:\Documents and Settings\All Users\Application Data\Symantec\Norton AntiVirus Corporate Edition\7.5
7. Перезапустите клиента.

Переключение управляемого клиента в режим автономного клиента

1. Удалите Symantec AntiVirus Corporate Edition с клиентской рабочей станции.
2. С помощью редактора реестра удалите следующий ключ реестра:
   HKEY_LOCAL_MACHINE\Software\Intel\LANDesk\VirusProtect6
3. Переустановите Symantec AntiVirus Corporate Edition.
4. При запросе о сценарии установки (управляемого или автономного клиента), выберите вариант «Автономный».

Глава 2

Настройка системы Alert Management System

Эта глава содержит следующие разделы:

- Сведения о системе Alert Management System
- Каким образом работает система Alert Management System
- Настройка действий для предупреждений
- Работа с настроенными предупреждениями
- Работа с журналом системы Alert Management System
- Пересылка предупреждений с автономных клиентов

Сведения о системе Alert Management System

Система Alert Management System[2] (AMS[2]) обеспечивает возможность управления критическими и особыми ситуациями. AMS[2] позволяет работать с предупреждениями на поддерживаемых серверах NetWare, на серверах и рабочих станциях Windows NT/2000, а также на рабочих станциях Windows XP Home Edition/Professional и Windows 98/Me.

Система AMS[2] может создавать предупреждения следующих видов:

- Message box (вывод окна сообщения)
- Broadcast (рассылка широковещательного сообщения)
- Internet mail (отправка электронной почты)
- Page (отправка сообщения на пейджер)
- Run a program (запуск программы)
- Write to the Windows NT Event Log (занесение записи в журнал событий Windows NT)
- Send an SNMP trap (отправка ловушки SNMP)
- Load an NLM (загрузка NLM)

Примечание: Предупреждения, создаваемые в виде ловушек SNMP, могут передаваться на любые консоли управления SNMP. Для получения ловушек SNMP от Symantec AntiVirus Corporate Edition необходимо установить Symantec System Center и AMS[2]. (Система AMS[2] будет работать только на первичном сервере. Первичный сервер необходимо назначить с помощью Symantec System Center).

См. «Настройка действия Send SNMP Trap» на стр. 67.

Каким образом работает система Alert Management System

Предупреждения AMS[2] передаются от Symantec AntiVirus Corporate Edition компоненту AMS[2] с помощью службы Symantec AntiVirus Corporate Edition. На компьютере, использующем клиента Symantec AntiVirus Corporate Edition, служба Symantec AntiVirus Corporate Edition ожидает поток предупреждения, который запрашивает отправку предупреждения.

Создание таких потоков может быть вызвано следующими событиями:

- Изменение конфигурации
- Предупреждение по умолчанию
- Ошибка контрольной суммы файла
- Запуск или завершение работы Symantec AntiVirus Corporate Edition
- Запуск или завершение осмотра
- Обновление файла описаний вирусов
- Обнаружение вируса

Если вы настроили предупреждение для любого из перечисленных событий, то обнаружение такого события приведет к созданию нового потока. Поток запрашивает у службы Symantec AntiVirus Corporate Edition создание блока информации о вирусе, который затем пересылается родительскому серверу клиента. После получения блока информации о вирусе родительский сервер записывает его в журнал AMS^2. Затем информация о вирусе пересылается основному серверу, который вызывает AMS^2. AMS^2 вводит информацию в базу данных AMS^2 и выполняет необходимые действия. Действия зависят от конфигурации предупреждений.

Связь в AMS осуществляется с помощью CBA, входящего в состав комплекса связи Intel Communication Method.

Настройка действий для предупреждений

Система AMS^2 позволяет использовать различные способы уведомления об обнаружении вирусов и изменении конфигурации, включая пейджинговые сообщения, SNMP и электронную почту.

Задачи настройки предупреждений

Для настройки предупреждения системы AMS^2 необходимо выполнить три связанных между собой задачи:

- Выбрать предупреждение в окне диалога «Alert Actions».
- Выбрать действие, которое необходимо настроить для этого предупреждения. Это действие будет ответом системы AMS^2 на обнаружение параметра, вызывающего отправку предупреждения.
- Настроить выбранное действие.

Например, можно настроить отправку сообщения на пейджер в случае обнаружения вируса на защищенном сервере. Пейджинговое сообщение может содержать также сведения об имени и типе вируса, и о том, какие действия были применены к зараженному файлу.

По умолчанию никакие действия для предупреждений не заданы. До тех пор, пока вы не настроите AMS^2, предупреждения формироваться не будут, хотя соответствующие сведения об обнаружении вирусов будут записываться в файл журнала AMS^2.

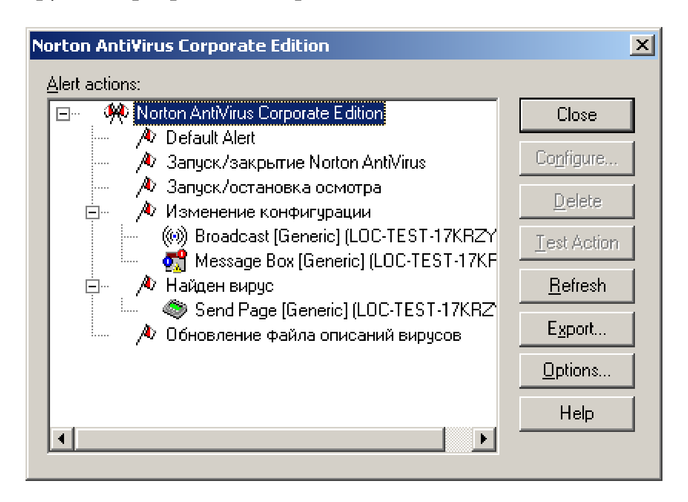
Для каждого предупреждения можно настроить несколько действий. После настройки действий рядом с этим предупреждением появляется знак «+» или «-», в зависимости от того, раскрыта ли запись.

Для каждого действия в системе AMS^2 предусмотрен отдельный мастер настройки. После настройки действия для предупреждения, это действие появляется в окне «Alert Actions» под соответствующим предупреждением.

Все действия выполняются на том компьютере, который был выбран при настройке действия. Действия не будут выполняться, если для их выполнения задан компьютер, не поддерживающий такие действия. Например, любой компьютер, указанный для отправки сообщений на пейждер, должен быть оснащен модемом.

Настройка предупреждения

1 В консоли Symantec System Center щелкните правой кнопкой мыши на группе серверов и выберите команды **Все задачи** > **AMS** > **Настроить**.



2 Выберите предупреждение и нажмите кнопку **Configure**, чтобы настроить для него действие.

Настройка сообщений в качестве действий

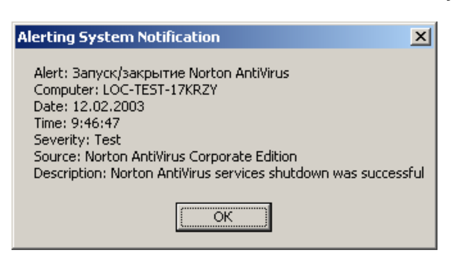
Если действие для предупреждения связано с созданием сообщения (например, окна сообщения, широковещательного сообщения, сообщения на пейджер и почтового сообщения), то в это сообщение можно включить дополнительную информацию о вызвавшем его событии. Дополнительные типы информации перечислены в Табл. 2-1.

Табл. 2-1 Параметры предупреждений

Параметр предупреждения	**Описание**
<Alert name>	Название предупреждения, например, запуск или завершение работы Symantec AntiVirus Corporate Edition.
<Computer>	Имя компьютера, сформировавшего данное предупреждение.
<Date>	Дата создания предупреждения.
<Description>	Дополнительная информация о предупреждении, например, «Работа служб Symantec AntiVirus Corporate Edition завершена успешно».
<Host Name>	Имя сервера предупреждений.
<Severity>	Уровень серьезности события, вызвавшего предупреждение, например, критическое или некритическое.
<Source>	Продукт, создавший предупреждение, например, Symantec AntiVirus Corporate Edition.
<Time>	Время создания предупреждения.

В окне сообщения предусмотрено текстовое поле, в котором можно ввести до 256 знаков текста передаваемого сообщения. Для вставки в сообщение информации о предупреждении можно воспользоваться значениями, перечисленными в поле «Alert Parameters». Параметры обозначаются символами < и >. Все указанные в тексте сообщения параметры при создании предупреждения заменяются соответствующими данными, как показано на Рис. 2-1.

Рис. 2-1 Сообщение системы управления предупреждениями



См. «Тестирование настроенных предупреждений» на стр. 70.

Если система AMS[2] обнаружит сообщение, размер которого превышает 1 Кб, то это сообщение не будет отправлено. Если было настроено сообщение по умолчанию, то оно будет отправлено вместо слишком большого сообщения. Можно настроить сообщение по умолчанию для уведомления о сообщениях, объем которых превышает 1 Кб.

Настройка предупреждающего сообщения по умолчанию

1. В консоли Symantec System Center щелкните правой кнопкой мыши на группу серверов и выберите команды **Все задачи** > **AMS** > **Настройка**.
2. Выберите **Default Alert** и нажмите кнопку **Configure**.
3. Выберите действие **Message** и нажмите кнопку **Next**.
4. Выберите компьютер, который будет выполнять это действие, и нажмите кнопку **Next**.
5. Укажите, следует ли подавать звуковой сигнал и должно ли окно оставаться поверх остальных окон, пока оно не будет закрыто пользователем.
6. Нажмите кнопку **Next**.
7. Укажите имя действия, описывающее настроенное сообщение.

   Имя действия и имя компьютера, выполняющего это действие, будут показаны в окне диалога «Alert Actions» после названия действия.
8. В поле сообщения введите одно из следующих значений:
   - Введите собственное сообщение, которое будет отображаться на экране, и добавьте в него любые параметры, перечисленные в поле «Alert Parameters».

- Для того чтобы в данном действии применялось сообщение по умолчанию, выберите параметр **Default** и укажите текст для вывода на экран.

  Сообщение по умолчанию включает следующую информацию:

  Компьютер: <Host Name>

  <Host Name> — это имя сервера предупреждений. Чтобы включить в сообщение имя компьютера, ставшего источником уведомления, необходимо добавить параметр <Computer>.

9 Нажмите кнопку **Finish**.

Ускорение настройки предупреждений с помощью дополнительных параметров обнаружения

В большой сети можно добиться ускорения и упрощения настройки системы AMS^2 путем использования дополнительных параметров обнаружения, чтобы ограничить область поиска компьютеров AMS^2 определенным сегментом сети.

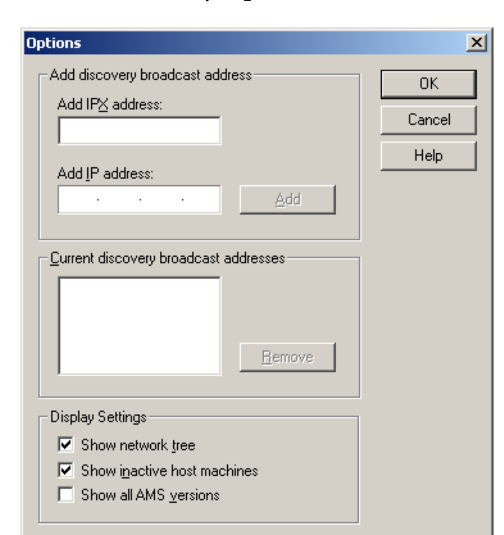
Эта возможность особенно полезна при управлении большой сетью, когда требуется ограничить область поиска одним сегментом сети или определенной маской подсети. Процесс обнаружения выполняется быстрее, если область поиска ограничена, а все предупреждения содержатся в пределах заданного сегмента сети.

Если ограничить эти сегменты, то можно получить более быстрые ответы при выполнении обнаружения для системы AMS^2 в большой сети. Эту возможность можно использовать как с протоколом IPX, так и с TCP/IP. Имеется возможность настроить систему AMS^2 на обнаружение клиентов только в пределах определенного октета или маски подсети.

Настройка дополнительных параметров обнаружения

1 В консоли Symantec System Center щелкните правой кнопкой мыши на группе серверов и выберите команды **Все задачи** > **AMS** > **Настроить**.

2 Нажмите кнопку **Options**.



3 В окне параметров выполните одно из следующих действий:

- Если в сети используется протокол IPX, то в поле «Add IPX address» введите широковещательный адрес IPX, по которому следует искать компьютеры AMS^2.
- Если в сети используется протокол TCP/IP, то в поле «Add IP address» введите широковещательный адрес TCP/IP, по которому следует искать компьютеры AMS^2.

  Этот адрес состоит из трех первых сегментов IP-адреса компьютера, после которых следует ограничивающий сегмент. Например, если ввести широковещательный адрес 192.168.0.255, то любой компьютер AMS^2, имеющий один из 256 адресов этой подсети, получит широковещательный запрос. Таким образом, если вы искали компьютер AMS^2 с IP-адресом 192.168.0.50, то этот компьютер будет найден.

4 Для добавления адреса в список «Current Discovery Broadcast Addresses» нажмите кнопку **Add**.

Обнаружение новых компьютеров AMS^2 будет осуществляться только в указанных в этом списке широковещательных диапазонах. Если широковещательные адреса не указаны, то при каждом запуске обнаружения поиск будет выполняться во всей сети.

5 Для того чтобы удалить ненужный сетевой адрес из списка «Current Discovery Broadcast Addresses», выберите адрес и нажмите кнопку **Remove**.

При удалении сетевого адреса из списка соответствующий сегмент сети не отключается. Удаление сетевого адреса только исключает этот сегмент сети из области поиска компьютеров AMS^2.

6 Нажмите кнопку **OK**, чтобы сохранить список и вернуться к окну диалога «Alert Actions».

Настройка действия Message Box

Действие «Message Box» выводит сообщение на экран того компьютера, с которого это действие было настроено. Вы можете указать, следует ли подавать звуковой сигнал при появлении сообщения и должно ли окно сообщения оставаться поверх остальных окон до тех пор, пока оно не будет закрыто пользователем.

Настройка действия Message Box

1. В консоли Symantec System Center щелкните правой кнопкой мыши на группе серверов и выберите команды **Все задачи** > **AMS** > **Настроить**.
2. Выберите предупреждение, для которого будет настраиваться действие.
3. Нажмите кнопку **Configure**.
4. Выберите действие **Message Box** и нажмите кнопку **Next**.
5. Выберите компьютер, который будет выполнять это действие, и нажмите кнопку **Next**.
6. Укажите, следует ли подавать звуковой сигнал и должно ли окно оставаться поверх остальных окон, пока оно не будет закрыто пользователем.
7. Нажмите кнопку **Next**.
8. Введите имя действия.

   Имя действия и имя компьютера, выполняющего это действие, будут показаны в окне диалога «Alert Actions» после названия действия.
9. Введите текст сообщения для вывода на экран, добавив в него любые параметры, перечисленные в поле «Alert Parameters».
10. Нажмите кнопку **Finish**.

Настройка действия Broadcast

Действие «Broadcast» рассылает сообщение всем компьютерам, подключенным к серверу, рассылающему предупреждения.

Настройка действия Broadcast

1. В консоли Symantec System Center щелкните правой кнопкой мыши на группе серверов и выберите команды **Все задачи** > **AMS** > **Настроить**.
2. Выберите предупреждение, для которого будет настраиваться действие.
3. Нажмите кнопку **Configure**.
4. Выберите действие **Broadcast**, и нажмите кнопку **Next**.
5. Выберите компьютер, который будет выполнять это действие, и нажмите кнопку **Next**.
6. Введите текст сообщения для вывода на экран, добавив в него любые параметры, перечисленные в поле «Alert Parameters».
7. Введите имя действия.

   Имя действия и имя компьютера, выполняющего это действие, будут показаны в окне диалога «Alert Actions» после общего названия действия.
8. Нажмите кнопку **Finish**.

Настройка действия Run Program

Действие «Run Program» запускает заданную программу на том компьютере, для которого это действие было настроено. В окне диалога «Run Program» необходимо заполнить два поля.

Поле «Program» должно содержать полный путь к запускаемой программе. В поле «Command Line» следует ввести параметры командной строки, необходимые для запуска этой программы. Система AMS^2 может работать только с программами, которые находятся на локальном диске компьютера.

Если программа запускается на удаленном компьютере, то необходимо указать путь к программе для этого компьютера.

Если запускается программа Windows, то можно выбрать режим запуска: нормальный, в свернутом окне или во весь экран. На программы DOS этот параметр не влияет.

Настройка действия Run Program

1. В консоли Symantec System Center щелкните правой кнопкой мыши на группе серверов и выберите команды **Все задачи** > **AMS** > **Настроить**.
2. Выберите предупреждение, для которого будет настраиваться действие.
3. Нажмите кнопку **Configure**.
4. Выберите действие **Run Program**, и нажмите кнопку **Next**.
5. Выберите компьютер, который будет выполнять это действие, и нажмите кнопку **Next**.
6. Укажите полный путь к программе, которую требуется запустить, включая имя файла.
7. Введите параметры командной строки, которые требуется использовать при запуске программы.
8. Выберите режим запуска: в нормальном окне, в свернутом окне или во весь экран.
9. Нажмите кнопку **Finish**.

Настройка действия Load NLM

Действие «Load An NLM» загружает модуль NetWare NLM на выбранном сервере NetWare при получении предупреждения AMS^2. При настройке этого действия необходимо указать, какой модуль NLM следует загружать, и на каком сервере это должно происходить. Это действие соответствует действию «Run Program» для компьютеров Windows NT.

Например, если вы используете модуль управления Symantec AntiVirus Corporate Edition, то вы можете настроить действие «Load An NLM» для загрузки созданного вами или другим производителем модуля NLM на выбранном сервере NetWare при обнаружении вируса программой Symantec AntiVirus Corporate Edition. Этот модуль NLM может контролировать доступ к серверу и проверять, кто обращается к зараженному файлу. Кроме того, он может создавать резервные копии файлов на случай сбоя сервера, вызванного заражением.

Настройка действия Load An NLM

1. В консоли Symantec System Center щелкните правой кнопкой мыши на группе серверов и выберите команды **Все задачи** > **AMS** > **Настроить**.
2. Выберите предупреждение, для которого будет настраиваться действие.
3. Нажмите кнопку **Configure**.
4. Выберите действие **Load An NLM**, и нажмите кнопку **Next**.

   При первой настройке этого действия система AMS^2 должна выполнить в сети поиск компьютеров NetWare, которые могут выполнить это действие.

   После завершения поиска найденные компьютеры NetWare будут представлены в виде иерархической структуры.
5. Если компьютер, который вы ищете, не показан в списке, то нажмите кнопку **Обнаружить** для повторного поиска всех компьютеров.
6. Выберите компьютер, на котором будет загружаться NLM, и нажмите кнопку **Next**.
7. Введите или выберите имя модуля NLM для загрузки.

   Модули NLM, как правило, хранятся на серверах NetWare в каталоге SYS:SYSTEM.
8. Введите параметры командной строки, которые требуется использовать при запуске программы.
9. Нажмите кнопку **Finish**.

Настройка действия Send Internet Mail

Действие «Send Internet Mail» отправляет сообщение по электронной почте указанному пользователю. При использовании действия «Send Internet Mail» необходимо указать почтовый сервер SMTP, через который будет осуществляться отправка сообщения. Если указывается имя почтового сервера, то в сети должен быть настроен сервер DNS, чтобы функция отправки почты могла определить IP-адрес этого сервера. Если сервер DNS отсутствует, то вместо имени следует указать IP-адрес почтового сервера.

Если в системе нет доступа к почтовому серверу SMTP, то это действие работать не будет.

Настройка действия Send Internet Mail

1. В консоли Symantec System Center щелкните правой кнопкой мыши на группе серверов и выберите команды **Все задачи** > **AMS** > **Настроить.**
2. Выберите предупреждение, для которого будет настраиваться действие.
3. Нажмите кнопку **Configure**.
4. Выберите действие **Send Internet Mail**, и нажмите кнопку **Next**.
5. Выберите компьютер, который будет выполнять это действие, и нажмите кнопку **Next**.
6. Укажите или выберите в соответствующих полях адрес, имя отправителя, тему сообщения и почтовый сервер.

   Для почтового сервера рекомендуется указывать IP-адрес, а не имя хоста.

   В поле имени отправителя должен быть указан действующий адрес электронной почты. Большинство почтовых серверов не отправляют сообщение, если не могут убедиться в существовании указанного адреса отправителя.
7. Нажмите кнопку **Next**.
8. В поле «Message» введите текст сообщения и добавьте в него любые параметры, представленные в поле «Alert Parameters».
9. Введите имя действия.

   Имя действия и имя компьютера, выполняющего это действие, будут показаны в окне диалога «Alert Actions» после названия действия.
10. Нажмите кнопку **Finish**.

Настройка действия Send Page

Действие «Send Page» отправляет сообщение на пейджер с указанным номером. К компьютеру, который будет отправлять сообщение на пейджер, должен быть подключен модем.

См. «Тестирование настроенных предупреждений» на стр. 70.

Настройка отправки сообщения на пейджер состоит из трех этапов:

- Настройка модема для его использования системой AMS[2]
- Настройка параметров пейджинговой службы
- Ввод пейджингового сообщения

Настройка действия Send Page

1. В консоли Symantec System Center щелкните правой кнопкой мыши на группе серверов и выберите команды **Все задачи** > **AMS** > **Настроить**.
2. Выберите предупреждение, для которого будет настраиваться действие.
3. Нажмите кнопку **Configure**.
4. Выберите действие **Send Page**, и нажмите кнопку **Next**.
5. Выберите компьютер, который будет выполнять это действие, и нажмите кнопку **Next**.
6. Укажите номер телефона пейджинговой компании.

   Помните о необходимости указать все необходимые коды для выхода из телефонной сети вашей организации на внешнюю линию.
7. Введите номер пейджера и пароль доступа к сети отправки сообщений.

   Если пейджинговая компания не использует пароли, оставьте поле пароля пустым.
8. Выберите тип пейджинговой службы.

   Если соответствующий тип отсутствует в списке, попробуйте использовать один из общих типов.

   См. «Настройка параметров пейджинговой службы» на стр. 65.
9. Нажмите кнопку **Next**.

   Если сообщение создается для алфавитно-цифрового пейджера, то в поле сообщения введите текст сообщения, добавив в него любые параметры, перечисленные в поле «Alert Parameters».

   Если сообщение создается для цифрового пейджера, то в поле сообщения можно вводить только цифры.
10. Введите имя действия.

    Имя действия и имя компьютера, выполняющего это действие, будут показаны в окне диалога «Alert Actions» после названия действия.
11. Нажмите кнопку **Finish**.

Настройка модема для системы AMS

Для того чтобы система AMS^2 могла обращаться к пейджинговой компании, необходимо настроить модем. Для правильной отправки сообщения на пейджер необходимо запустить программу настройки модема и выбрать последовательный (COM) порт и тип модема.

Настройка модема для системы AMS

1 Запустите утилиту настройки, дважды щелкнув на файле **Modemcfg.exe** в Проводнике.

  Эта программа установлена на компьютере, выполняющем действие, в папке Winnt\System32\AMS_ii.

2 Выберите последовательный (COM) порт, который использует модем.

3 Выберите тип модема.

4 Нажмите кнопку **OK**, чтобы сохранить эти параметры и завершить настройку модема для работы с системой AMS^2.

Настройка параметров пейджинговой службы

Доступ к услугам пейджинговой связи может осуществляться напрямую или через оператора. При прямом доступе требуется позвонить по номеру пейджинговой компании, выделенному для прямого доступа к ее компьютерной сети, передачи сообщения и указания номера абонента, для которого предназначено сообщение. После этого сообщение передается на пейджер.

Система AMS^2 не работает в режиме доступа к услугам через оператора. В режиме доступа через оператора необходимо позвонить в пейджинговую компанию, продиктовать сообщение оператору и назвать ему номер абонента, для которого предназначено сообщение. Оператор вводит сообщение через персональный компьютер в сеть, а затем это сообщение передается из сети компании на пейджер. Метод доступа через оператора часто используется в качестве бесплатной альтернативы прямому доступу, за который взимается плата.

Необходимо настроить параметры действия в соответствии с используемой пейджинговой службой. Как минимум, требуется указать телефонный номер для доступа к сети и название используемой пейджинговой службы.

Номер телефона пейджинговой службы должен быть обязательно указан в поле «Service Provider» окна диалога «Send Page». Если пейджинговая служба, которой вы пользуетесь, не указана в списке служб в окне диалога

«Send Page», то можно попробовать воспользоваться службой «Generic Beeper» или «Generic Alphanumeric» (в зависимости от типа используемого пейджера). Введите пароль для доступа к сети пейджинговой компании.

Если выбранная общая служба не работает с вашим пейджером, то необходимо настроить параметры связи, используемые при отправке сообщения на пейджер. К этим параметрам относятся скорость передачи данных, количество битов данных и стоповых битов, параметры контроля четности, а также протокол, используемый пейджинговой службой. Если служба, которой вы пользуетесь, есть в списке, то необходимые параметры автоматически настраиваются при выборе этой службы.

Настройка действия Send Page для служб, не указанных в списке

1. В консоли Symantec System Center щелкните правой кнопкой мыши на группе серверов и выберите команды **Все задачи** > **AMS** > **Настроить**.
2. Выберите предупреждение, для которого будет настраиваться действие.
3. Нажмите кнопку **Configure**.
4. Выберите действие **Send Page**, и нажмите кнопку **Next**.
5. Выберите компьютер, который будет выполнять это действие, и нажмите кнопку **Next**.
6. Нажмите кнопку **Settings**.
7. Укажите протокол, максимальную длину сообщения, скорость передачи данных, количество битов данных, стоповых битов и метода проверки четности, используемые пейджинговой службой.

   Эту информацию можно получить в пейджинговой компании.
8. Нажмите кнопку **OK**, затем продолжайте настройку действия с шага 6 инструкции в разделе «Настройка действия Send Page» на стр. 64.

Ввод сообщения для пейджера

Действие «Send Page» поддерживает как алфавитно-цифровые, так и только цифровые пейджеры (только цифровые пейджеры также называют «бипперами»).

Если вы пользуетесь алфавитно-цифровым пейджером, то передаваемое сообщение может содержать любой текст, а также и информацию о предупреждении. Во избежание получения неполных сообщений длина сообщения не должна превышать максимального числа знаков, поддерживаемого вашей пейджинговой службой.

При использовании цифрового пейджера рекомендуется создать систему нумерации серверов и цифровых кодов ошибок, соответствующих настроенным предупреждениям. Например, вы можете создать систему, в которой цифра «1» указывает на главный сервер, а число «101» соответствует определенному событию. В таком случае, получив сообщение «1 101», вы поймете, что на главном сервере произошло определенное событие.

Настройка действия Send SNMP Trap

Протокол SNMP (Simple Network Management Protocol – простой протокол управления сетью) является протоколом сообщений, основанным на модели «диспетчер-агент». В этом протоколе применяются сообщения и ответы Get, GetNext и Set. Протокол SNMP использует ловушки для сообщения об определенных состояниях, например, о сбоях компонентов и о превышении установленных пороговых значений.

Система AMS^2 может создать ловушку SNMP для рассылки предупреждений. Систему рассылки предупреждений можно настроить на передачу ловушек SNMP различным консолям управления, например, HP OpenView, Tivoli Enterprise Console или Computer Associates Unicenter.

Необходимо указать адреса (IP или IPX) компьютеров, которым требуется отправлять ловушки SNMP.

Настройка действия Send SNMP Trap

1. В консоли Symantec System Center щелкните правой кнопкой мыши на группе серверов и выберите команды **Все задачи** > **AMS** > **Настроить**.
2. Выберите предупреждение, для которого будет настраиваться действие.
3. Нажмите кнопку **Configure**.
4. Выберите действие **Send SNMP Trap**, и нажмите кнопку **Next**.
5. Выберите компьютер, который будет выполнять это действие, и нажмите кнопку **Next**.
6. В окне «SNMP Trap» введите текст сообщения, добавив в него любые параметры, перечисленные в поле «Alert Parameters».
7. Введите имя действия.

   Имя действия и имя компьютера, выполняющего это действие, будут показаны в окне диалога «Alert Actions» после названия действия.
8. Нажмите кнопку **Finish**.

Настройка получателей ловушек в Windows NT 4.0

Вы можете настроить ловушки SNMP для Windows NT 4.0.

Настройка получателей ловушек для Windows NT 4.0

1. В Панели управления Windows NT дважды щелкните на значке **Сеть.**
2. Выберите вкладку **Службы**.
3. Выберите запись **Служба SNMP** и нажмите кнопку **Свойства.**
4. Откройте вкладку **Ловушки.**
5. В группе «Имя сообщества» выберите сообщество **Public**.
6. Если сообщество «Public» в списке отсутствует, введите это название и нажмите кнопку **Добавить.**
7. Нажмите кнопку **Добавить**, находящуюся под полем «Адресаты ловушек».
8. Введите адреса компьютеров, которым требуется отправлять ловушки, и нажмите кнопку **Добавить.**
9. Нажмите кнопку **ОК**, а затем – кнопку **Закрыть**.

Настройка получателей ловушек в Windows 2000 Server

Вы можете настроить ловушки SNMP для Windows 2000 Server

Настройка получателей ловушек для Windows 2000 Server

1. На панели задач Windows выберите команды **Пуск** > **Настройка** > **Панель управления**.
2. Дважды щелкните на значке **Администрирование**.
3. Дважды щелкните на значке **Управление компьютером**.
4. Выберите **Службы и приложения.**
5. Выберите **Службы.**
6. В правой части окна выберите запись **Служба SNMP.**
7. В меню «Действие» выберите команду **Свойства.**
8. На вкладке «Ловушки» в разделе «Имя сообщества» введите имя сообщества, которому компьютер будет отправлять ловушки, и нажмите кнопку **Добавить в список**. Имена сообществ задаются с учетом регистра.

9 Нажмите кнопку **Добавить** в группе «Адресаты ловушек».

10 Введите информацию о хосте, задав его имя, адрес IP или адрес IPX, после чего нажмите кнопку **Добавить**.

11 Повторите шаги с 8 по 10, добавив все сообщества и всех получателей ловушек.

Настройка получателей ловушек для NetWare

Вы можете настроить ловушки SNMP для серверов NetWare 4.1x, 5.x, и 6.x.

Настройка получателей ловушек для NetWare

1 На консоли сервера NetWare введите:
load inetcfg

2 Выберите команду **Протоколы** и нажмите клавишу **Enter**.

3 Выберите команду **TCP/IP** и нажмите клавишу **Enter**.

4 Выберите команду **Таблица диспетчера SNMP** и нажмите клавишу **Enter**, чтобы вывести на экран таблицу диспетчера SNMP.

5 Выполните одно из следующих действий:

- Чтобы изменить существующий адрес, выберите его и нажмите клавишу **Enter**.
- Чтобы добавить новый адрес, нажмите клавишу **Insert**, введите IP-адрес и нажмите клавишу **Enter**.
- Чтобы удалить адрес, выберите его, нажмите клавишу **Delete**, а затем нажмите клавишу **Enter** для подтверждения удаления.

6 Нажмите клавишу **Esc**, чтобы закрыть окно.

7 Нажмите клавишу **Enter**, чтобы подтвердить изменение базы данных.

Настройка действия Write To Event Log

Действие «Write To Event Log» создает запись в журнале приложений Windows NT/2000/XP. Эта запись регистрируется на сервере, с которого пришло предупреждение. Это действие доступно только на компьютерах Windows NT/2000/XP.

Настройка действия Write To Event Log

1 В консоли Symantec System Center щелкните правой кнопкой мыши на группе серверов и выберите команды **Все задачи** > **AMS** > **Настроить.**

2. Выберите предупреждение, для которого будет настраиваться действие.
3. Нажмите кнопку **Configure**.
4. Выберите действие **Write To Event Log** и нажмите кнопку **Next**.
5. Выберите компьютер, который будет выполнять это действие, и нажмите кнопку **Next**.
6. Введите текст сообщения для вывода на экран, добавив в него любые параметры, перечисленные в поле «Alert Parameters».
7. Введите имя действия.

   Имя действия и имя компьютера, выполняющего это действие, будут показаны в окне диалога «Alert Actions» после названия действия.
8. Нажмите кнопку **Finish**.

Работа с настроенными предупреждениями

После настройки действий для предупреждений вы можете выполнить следующие операции:

- Протестировать предупреждения и проверить правильность их работы
- Удалить предупреждения
- Экспортировать предупреждения на другие компьютеры

Тестирование настроенных предупреждений

После настройки действий для предупреждений вы можете протестировать их с помощью окна «Alert Actions». Когда вы выбираете предупреждение и нажимаете кнопку «Test Action», выполняются все настроенные для этого предупреждения действия. Когда вы выбираете отдельное действие и нажимаете кнопку «Test Action», выполняется только это действие.

Тестирование предупреждения

- В окне «Alert Actions» выберите предупреждение и нажмите кнопку **Test Action**.

Удаление действия из предупреждения

При необходимости вы можете удалить действия, связанные с предупреждением.

Удаление действия из предупреждения

1. В консоли Symantec System Center щелкните правой кнопкой мыши на группе серверов и выберите команды **Все задачи** > **AMS** > **Настроить**.
2. Выберите действие, которое требуется удалить, и нажмите кнопку **Delete**.

Экспорт действия для предупреждений на другие компьютеры

Каждый компьютер, создающий предупреждения AMS^2, хранит информацию о своих предупреждениях в локальной базе данных AMS^2. Как правило, предупреждения и действия, хранящиеся на одном компьютере, недоступны для баз данных AMS^2 других компьютеров.

Возможно, вы захотите скопировать настройку действий системы AMS^2 с одного компьютера на другие, не повторяя уже проделанной работы. Функция экспорта, имеющаяся в системе AMS^2, позволяет переносить настройку действий для предупреждений на другие компьютеры, передающие предупреждения AMS^2.

Действия для предупреждений, такие как «Send Page» или «Message Box» экспортируются только в том случае, если предупреждение, для которого настроены эти действия, существуют на обоих компьютерах. В большинстве случаев это обеспечивается установкой одинаковых приложений на оба компьютера. В этом случае оба приложения зарегистрируют свои предупреждения в соответствующих базах данных AMS^2.

При экспорте действий для предупреждений с одного компьютера на другой имеется возможность экспортировать как отдельное действие, так и все действия. Завершив экспорт данных на другой компьютер, система AMS^2 выводит на экран окно «Export Status», сообщающее о результатах экспорта.

Если функция экспорта не смогла экспортировать действие из-за того, что предупреждение, для которого это действие настроено, не существует на другом компьютере (или по другой причине), то сообщение об этом появится в окне «Export Status». Возникновение сбоев при экспорте действий возможно также в том случае, если система AMS^2 на другом компьютере работает неправильно.

Экспорт действий для предупреждений на другие компьютеры

1. В консоли Symantec System Center щелкните правой кнопкой мыши на группе серверов, а затем выберите команды **Все задачи** > **AMS** > **Настроить**.
2. Выполните одно из следующих действий:
   - Если необходимо экспортировать все предупреждения, связанные с Symantec AntiVirus Corporate Edition, то выберите папку **Norton AntiVirus Corporate Edition**.
   - Выберите либо предупреждение (чтобы экспортировать все действия этого предупреждения), либо отдельное действие (чтобы экспортировать только это действие).
3. Нажмите кнопку **Export**.
4. В списке доступных компьютеров дважды щелкните на компьютерах, которым должны передаваться выбранные действия для предупреждений.

   Эти компьютеры будут добавлены в список выбранных компьютеров.

   Если на нужном компьютере работает система AMS^2, но он отсутствует в списке доступных компьютеров, то для повторного обнаружения компьютеров с системой AMS^2 нажмите кнопку **Обнаружить**.
5. Нажмите кнопку **Export**.
6. Нажмите кнопку **Yes** в окне подтверждения.
7. В окне состояния экспорта проверьте, успешно ли завешен экспорт действий для предупреждений.

Просмотр данных о состоянии экспорта

После того, как AMS^2 экспортирует действия для предупреждений на выбранные компьютеры, система AMS^2 сообщает о результатах экспорта с помощью окна состояния экспорта.

В окне состояния экспорта указаны действия для предупреждений, которые не удалось экспортировать. Если экспортировать предупреждения не удалось, это может быть вызвано следующими причинами:

- Система AMS^2 на другом компьютере не запущена или работает неправильно. Проверьте правильность работы системы AMS^2 путем тестирования настроенного действия на этом компьютере с помощью окна «Действия для предупреждений».

- Предупреждение, для которого было настроено это действие, не существует на другом компьютере. Убедитесь в том, что приложение, зарегистрировавшее предупреждение в системе AMS^2 компьютера-источника, установлено на компьютере-получателе.

Работа с журналом системы Alert Management System

В журнале предупреждений хранится список всех предупреждений, созданных сетевыми компьютерами Symantec AntiVirus Corporate Edition.

Журнал предупреждений может работать в следующих режимах:

- Отображение только предупреждений, отвечающих заданным критериям.
- Отображение только указанного количества записей.

В журнале предупреждений отображается список предупреждений с указаний следующих данных для каждого предупреждения.

- Alert Name (название предупреждения)
- Source (источник)
- Computer (компьютер)
- Date (дата)
- Time (время)
- Severity (важность)

Кроме этой основной информации, представленной в окне журнала предупреждений, есть возможность просмотреть более подробные сведения в окне информации о предупреждении.

На каждом сервере хранится собственная локальная копия журнала предупреждений. Когда вы выбираете сервер и просматриваете его журнал предупреждений, то фактически в локальную консоль загружается копия журнала с этого сервера. Таким образом, если сервер выключен или не доступен, вы не сможете получить его журнал предупреждений для просмотра.

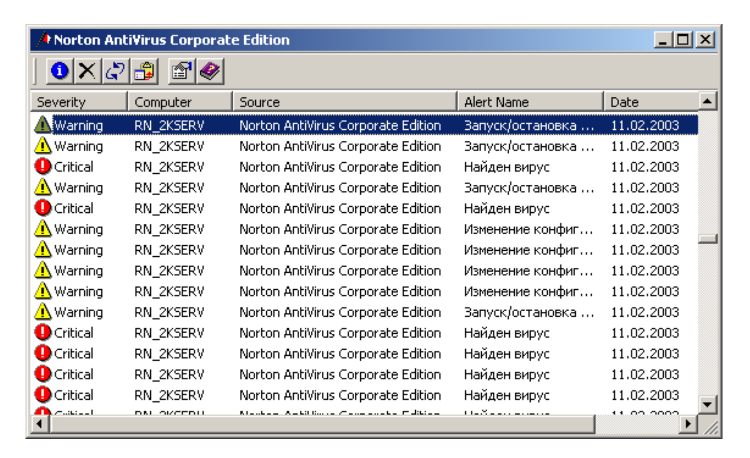
Просмотр журнала предупреждений и работа с ним

Вы можете просматривать журнал предупреждений и выполнять с ним следующие операции:

- Изменение числа показанных записей журнала
- Удаление записей
- Копирование содержимого в буфер обмена

Просмотр журнала предупреждений

- ◆ Щелкните правой кнопкой мыши на группе серверов и выберите команды **Все задачи** > **AMS** > **Просмотр журнала.**



Изменение числа записей, отображаемых в журнале предупреждений

1 Щелкните правой кнопкой мыши в окне журнала предупреждений и выберите команду **Options**.

2 Укажите количество записей, которые требуется хранить в журнале.

Примечание: Количество записей журнала можно настроить отдельно для каждого сервера.

Удаление отдельной записи журнала

- ◆ Щелкните правой кнопкой мыши на удаляемой записи журнала и команды **Delete** > **Selected Entries.**

Удаление нескольких записей журнала

1 Удерживая нажатой клавишу **Ctrl**, выберите несколько записей журнала.

2 Щелкните правой кнопкой мыши в окне журнала предупреждений и выберите команды **Delete** > **Selected Entries**.

Для выбора нескольких соседних записей щелкните на первой записи, затем нажмите клавишу **Shift** и, удерживая ее, щелкните на последней записи.

Удаление всех показанных записей журнала

◆ Щелкните правой кнопкой мыши в окне журнала предупреждений и выберите команды **Delete** > **Filtered Entries**.

Копирование содержимого журнала предупреждений в буфер обмена

1 Удерживая нажатой клавишу **Ctrl**, выберите несколько записей журнала.

2 Щелкните правой кнопкой мыши в окне журнала предупреждений и выберите команду **Copy**.

Копируются только записи, показанные в списке. Для того чтобы ограничить число копируемых в буфер обмена записей журнала, примените фильтры для отображения только определенных записей.

Просмотр подробных сведений о предупреждении

Вы можете просмотреть подробные сведения о каждом записанном в журнал предупреждении. Эти сведения отображаются в окне информации о предупреждении и включают в себя предупреждения, их параметры и результат выполнения действий для каждого предупреждения.

В окне отображается список параметров, например, название предупреждения, источник, дата, важность и описание, а также их значения для выбранного предупреждения.

В окне информации о предупреждении также указываются типы состояния, перечисленные в Табл. 2-2.

Табл. 2-2 Типы состояния действий

Состояние действия	Описание
Action Type	Тип действия, выполненного для предупреждения, например, вывод окна сообщения, отправка сообщения на пейджер, отправка электронной почты, запуск программы или рассылка широковещательного сообщения.
Action Name	Имя, присвоенное конкретному действию.
Computer	Имя компьютера, создавшего предупреждение.
Status	Состояние предупреждения. Возможны следующие состояния: ожидание (pending), обработка действия (processing), ошибка (error), успешное завершение (completed successfully) и неудачное завершение (failed to complete).

Просмотр сведений о предупреждении и состоянии действия

1 В окне журнала предупреждений дважды щелкните на предупреждении, для которого необходимо просмотреть подробные сведения.

2 Закончив просмотр сведений о предупреждении, нажмите кнопку **Close**.

   Компьютер, указанный в окне журнала предупреждений, — это всегда первичный сервер, зарегистрировавший предупреждение, поскольку он записывает все события для группы серверов Symantec. Чтобы увидеть, какой компьютер создал предупреждение, дважды щелкните на интересующей вас записи журнала предупреждений. В окне информации о предупреждении будут показаны более подробные сведения о предупреждении, в том числе и имя компьютера, создавшего предупреждение.

Применение фильтров для списка журнала предупреждений

Вы можете включить в показанный список предупреждений только те предупреждения, которые отвечают определенным критериям.

Фильтровать показанные предупреждения можно с помощью параметров, перечисленных в Табл. 2-3.

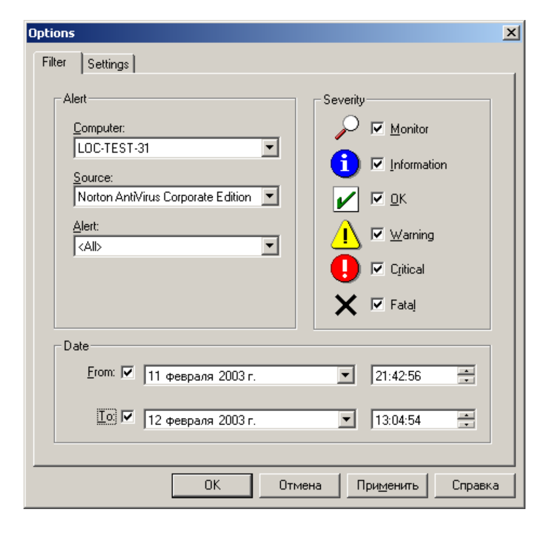
Табл. 2-3 Фильтры журнала предупреждений

Фильтр	Описание
Computer	Отображаются только предупреждения от определенного компьютера.
Source	Отображаются только предупреждения от источников одного типа с одного или нескольких компьютеров.
Alert	Отображаются все предупреждения с определенным названием.
Severity	Отображаются только предупреждения с выбранным уровнем важности. Можно указать следующие уровни: Monitor, Information, OK, Non-critical, Critical, и Non-recoverable.

Выбор предупреждений для отображения в журнале

1 В консоли Symantec System Center щелкните правой кнопкой мыши на группе серверов и выберите **Все задачи** > **AMS** > **Просмотр журнала.**

2 Щелкните правой кнопкой мыши в окне журнала предупреждений и выберите команду **Options**.



3 Выберите фильтры, которые нужно применить к списку журнала предупреждений.

4 Нажмите кнопку **OK**.

Пересылка предупреждений с автономных клиентов

Вы можете настроить автономные клиенты Symantec AntiVirus Corporate Edition для пересылки предупреждений серверу AMS^2.

Для отправки предупреждения клиентский компьютер должен быть подключен к сети и у него должна быть возможность подключения к серверу AMS.

Пересылка предупреждений серверу AMS

1 С помощью текстового редактора, например, Блокнота, создайте новый текстовый файл.

2 Добавьте в файл следующие строки:

```
[KEYS]
!KEY!=$REGROOT$\Common
AMSServer=S<AMSServerName>
AMS=D1
!KEY!=$REGROOT$\ProductControl
LoadAMS=D1
```

3 Замените слово <AMSServerName> одним из следующих значений:

- IP или IPX-адрес назначаемого сервера AMS^2.
- Имя назначаемого сервера AMS^2 (убедитесь в том, что клиент сможет распознать имя сервера).

  Не забудьте указать букву S перед значением <SERVERNAME>. Не заключайте имя сервера в скобки.

4 Сохраните файл под именем Grc.dat в следующей папке автономного клиента:

- В системах Windows 98\Me: C:\Program Files\Norton AntiVirus
- В системах Windows NT: C:\Winnt\Profiles\All Users\Application Data\Symantec\Norton AntiVirus Corporate Edition\7.5
- В системах Windows 2000\XP: C:\Documents and Settings\All Users\Application Data\Symantec\Norton AntiVirus Corporate Edition\7.5

Создав файл конфигурации (Grc.dat), вы можете копировать его на другие автономные клиенты. Эти автономные клиенты также смогут пересылать предупреждения на тот же сервер AMS^2.

Раздел 2

Настройка Symantec AntiVirus Corporate Edition

Глава 3

Проверка на наличие вирусов

Эта глава содержит следующие разделы:

Сведения об осмотрах Symantec AntiVirus Corporate Edition

С помощью консоли Symantec System Center можно настроить четыре типа осмотров:

- Осмотры постоянной защиты
- Плановые осмотры
- Ручные осмотры
- Осмотр вложений в сообщения электронной почты Lotus Notes, Microsoft Exchange и Outlook (MAPI)

При этом возможны следующие способы осмотра:

- Осмотр одного или нескольких серверов и клиентов Symantec AntiVirus Corporate Edition
- Осмотр групп серверов и клиентов Symantec AntiVirus Corporate Edition с помощью групп серверов

Постоянная защита

Постоянная защита обеспечивает непрерывную проверку файлов и сообщений электронной почты, принимаемых и передаваемых компьютером. Постоянная защита по умолчанию включена. Параметры постоянной защиты для серверов можно настраивать на уровне сервера или группы серверов, а для клиентов — на уровне сервера, группы серверов и на уровне группы клиентов. При настройке параметров постоянной защиты файловой системы страницы настройки серверов и клиентов несколько отличаются друг от друга. Кроме того, для реализации определенной политики защиты от вирусов вы можете заблокировать параметры постоянной защиты клиентов. Пользователи не смогут изменить заблокированные вами параметры.

Symantec AntiVirus Corporate Edition проверяет данные сообщений электронной почты только на клиентах Symantec AntiVirus Corporate Edition.

Плановые осмотры

С помощью консоли Symantec System Center можно запланировать сеансы осмотра для серверов и клиентов Symantec AntiVirus Corporate Edition. Пользователи также могут настраивать плановые осмотры на клиентах

Symantec AntiVirus Corporate Edition, но они не могут изменять или отключать осмотры, запланированные вами. Symantec AntiVirus Corporate Edition в каждый момент времени может выполнять один запланированный осмотр. Если на одно и то же время запланировано несколько сеансов осмотра, они будут выполняться последовательно.

Когда вы создаете и сохраняете плановый осмотр, Symantec AntiVirus Corporate Edition запоминает, для какой группы серверов, сервера или компьютера создан осмотр, а также сохраняет параметры, выбранные вами для этого осмотра.

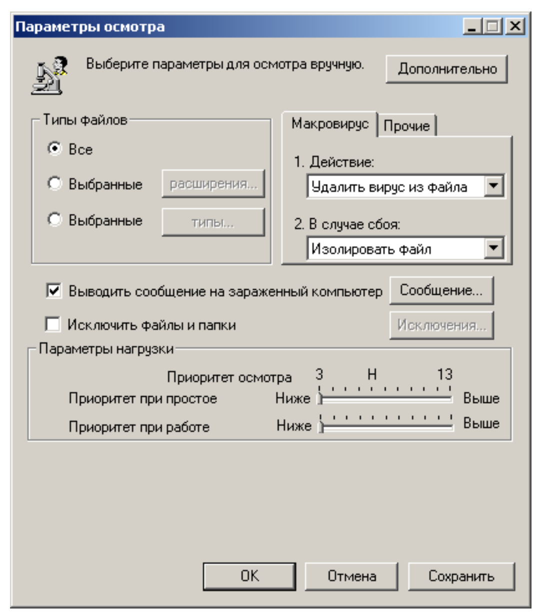
Если в момент осмотра компьютер выключен и обработка пропущенных событий не настроена, то осмотр выполнен не будет.

См. «Настройка обработки пропущенных плановых осмотров» на стр. 101.

Ручные осмотры

При осмотре вручную (ручной осмотр по требованию) проверяются выбранные файлы и папки на выбранных компьютерах. Ручной осмотр оптимален для быстрой проверки небольших областей сети или локального жесткого диска. Параметры осмотра можно задать с помощью окна диалога, показанного на Рис. 3-1.

Рис. 3-1 Окно параметров осмотра



Выбор компьютеров для осмотра

В Symantec System Center необходимо выбрать компьютеры для осмотра, задать тип осмотра, а также указать, где должен выполняться осмотр и настроить параметры осмотра.

Табл. 3-1 содержит список типов объектов, для которых может выполняться осмотр.

Табл. 3-1 Объекты для осмотра

Выбранный объект	Доступные виды просмотра
Структура системы	Сплошная проверка всех серверов и клиентов Symantec AntiVirus Corporate Edition в сети.
Несколько групп серверов	■ Сплошная проверка всех серверов и клиентов Symantec AntiVirus Corporate Edition, входящих в выбранные группы серверов. ■ Плановый осмотр выбранных серверов Symantec AntiVirus Corporate Edition.
Группа серверов	■ Сплошная проверка всех серверов и клиентов Symantec AntiVirus Corporate Edition, входящих в выбранную группу серверов. ■ Плановый осмотр серверов Symantec AntiVirus Corporate Edition, входящих в выбранную группу.
Серверы в группе серверов	■ Сплошная проверка выбранных серверов Symantec AntiVirus Corporate Edition. ■ Ручной осмотр выбранных серверов Symantec AntiVirus Corporate Edition.
Отдельный сервер	■ Сплошная проверка сервера Symantec AntiVirus Corporate Edition и всех его клиентов Symantec AntiVirus Corporate Edition. ■ Ручной осмотр сервера Symantec AntiVirus Corporate Edition. ■ Плановый осмотр сервера Symantec AntiVirus Corporate Edition и всех его клиентов Symantec AntiVirus Corporate Edition.
Клиенты Symantec AntiVirus Corporate Edition отдельного сервера Symantec AntiVirus Corporate Edition	Ручной осмотр выбранных клиентов Symantec AntiVirus Corporate Edition, управляемых сервером Symantec AntiVirus Corporate Edition.

Табл. 3-1 Объекты для осмотра

Выбранный объект	Доступные виды просмотра
Отдельный клиент Symantec AntiVirus Corporate Edition	■ Ручной осмотр выбранного клиента Symantec AntiVirus Corporate Edition. ■ Плановый осмотр выбранного клиента Symantec AntiVirus Corporate Edition.

Примечание: Для передачи клиентам настроенных с помощью консоли Symantec System Center параметров постоянной защиты параметры настройки клиентов должны быть заблокированы.

См. «Настройка постоянной защиты» на стр. 86.

Определение параметров осмотра для нескольких компьютеров

При просмотре параметров постоянной защиты, сплошной проверки или ручного осмотра для нескольких выбранных компьютеров, флажки и параметры могут находиться в третьем состоянии, которое говорит о том, что компьютеры имеют разные значения этих параметров. Для просмотра разных состояний параметра щелкните на этом параметре несколько раз.

- Сплошной черный цвет флажка или переключателя говорит о том, что этот параметр выбран на всех компьютерах группы. Установка параметра в состояние иное, чем обозначенное серым цветом, изменяет настройку этого параметра для всех выбранных компьютеров.
- Снятый флажок означает, что параметр выключен на всех выбранных компьютерах. Установка параметра в состояние иное, чем обозначенное серым цветом, изменяет настройку этого параметра для всех выбранных компьютеров.
- Серый флажок или переключатель, пустое поле или пустой набор параметров означает, что на некоторых из выбранных компьютеров эти параметры включены, а на некоторых — выключены. Установка параметра в состояние иное, чем обозначенное серым цветом, изменяет настройку этого параметра для всех выбранных компьютеров.

Некоторые параметры, например, исключение файлов и папок, недоступны, когда выбрано несколько компьютеров, поскольку эти параметры можно применить только к отдельному компьютеру.

Приоритет параметров осмотра

Изменения, внесенные в параметры осмотра на уровне группы серверов, имеют более высокий приоритет, чем изменения, внесенные на уровне группы клиентов или на уровне отдельного сервера.

Примечание: Параметры постоянной защиты несколько отличаются от параметров других осмотров. Для передачи клиентам параметров постоянной защиты эти параметры должны быть заблокированы на уровне группы серверов или на уровне отдельного сервера.

См. «Постоянная защита» на стр. 82.

Настройка постоянной защиты

Для настройки осмотров постоянной защиты необходимо выполнить следующие задачи:

- Настройка постоянной защиты для файлов
- Настройка постоянной защиты электронной почты
- Настройка исключений
- Передача параметров постоянной защиты подключенным к сети группам серверов, отдельным серверам Symantec AntiVirus Corporate Edition и клиентам Symantec AntiVirus Corporate Edition

Настройка постоянной защиты для файлов

При настройке постоянной защиты для файлов необходимо выбрать отдельный сервер или группу серверов для осмотра, и указать обычные и дополнительные параметры осмотра.

Настройка постоянной защиты для файлов

1 Выполните одно из следующих действий:

- Щелкните правой кнопкой мыши на настраиваемом сервере или группе серверов Symantec AntiVirus Corporate Edition, и выберите команды **Все задачи** > **Symantec AntiVirus** > **Параметры постоянной защиты сервера**.

  Если выбрана группа серверов, то Symantec System Center полагает, что вы хотите настроить все серверы, входящие в эту группу.

- Щелкните правой кнопкой мыши на отдельном сервере или на нескольких выбранных серверах, и выберите команды **Все задачи** > **Symantec AntiVirus** > **Параметры постоянной защиты клиента**.
- Щелкните правой кнопкой мыши на сервере или группе серверов с настраиваемыми клиентами Symantec AntiVirus Corporate Edition, и выберите команды **Все задачи** > **Symantec AntiVirus** > **Параметры постоянной защиты клиента**.

  Symantec System Center настроит всех клиентов, связанных с выбранным сервером или с группой серверов.
- Щелкните правой кнопкой мыши на отдельном клиенте или на нескольких выбранных клиентах сервера, и выберите команды **Все задачи** > **Symantec AntiVirus** > **Параметры постоянной защиты клиента**.

2. В окне параметров постоянной защиты клиента должен быть установлен флажок **Постоянная защита файловой системы**.
3. Настройте параметры постоянной защиты.

   Вы можете:
   - Выбрать файлы для осмотра по типам и по расширениям
   - Назначить первичные и вторичные действия, выполняемые при обнаружении вирусов
   - Настроить вывод сообщения на экран зараженного компьютера
   - Исключить файлы и папки из списка осмотра
   - Выбрать типы дисков для осмотра
4. Нажмите кнопку **Дополнительно**.

   Вы можете:
   - Включить осмотр измененных или просмотренных файлов.
   - Включить создание резервных копий файлов перед попыткой их исправления, чтобы предотвратить возможную потерю данных. Файлы будут зашифрованы и помещены в специальную папку в изоляторе. После создания резервной копии файла для доступа к нему необходимо восстановить этот файл.
   - Указать, нужно ли проверять сжатые файлы на серверах. По умолчанию сжатые файлы на серверах не проверяются. Если проверка включена, можно задать уровень распаковки вложенных архивов. По умолчанию задана проверка до 3 уровней вложенности.

На серверах NetWare Symantec AntiVirus Corporate Edition максимальный уровень вложенности при проверке сжатых файлов равен трем.

5. Для изменения уровня чувствительности защиты с помощью эвристической технологии Bloodhound нажмите кнопку **Эвристика**.

   Технология Bloodhound позволяет обнаружить большинство неизвестных вирусов путем изолирования и выделения логических областей файла. После этого технология Bloodhound анализирует логику работы программы и выявляет признаки вирусоподобных действий.

6. Выбрав необходимые значения, нажмите кнопку **OK**.

7. Для изменения текущих параметров проверки гибких дисков нажмите кнопку **Дискеты**.

   Выберите один из следующих вариантов:

   - Проверять загрузочный сектор дискет при обращении: При первом обращении к дискете Symantec AntiVirus Corporate Edition будет проверять наличие на этой дискете загрузочных вирусов. Укажите, какое действие следует выполнять при обнаружении загрузочного вируса: исправить загрузочную запись или оставить ее без изменений.

     Если выбрано действие «Не исправлять» то при обнаружении вируса будет отправляться предупреждение, однако действие выполнено не будет. Используйте этот параметр только в том случае, если вы хотите самостоятельно управлять процессом удаления вируса. Например, получив уведомление, вы можете решить, какие действия следует предпринять.

   - Не проверять дискеты при выходе из системы: При обычном завершении работы системы Symantec AntiVirus Corporate Edition не будет проверять находящиеся в дисководах дискеты.

8. В Windows 98 для выключения контроля выберите **Монитор**.

   Вирусоподобными называются действия, которые характерны для большинства вирусов, пытающихся заразить файлы. Однако такие действия могут являться и частью обычного рабочего процесса. Можно отключить отслеживание следующих действий:

   - Низкоуровневое форматирование: Вся содержащаяся на диске информация удаляется и не подлежит восстановлению. Такой тип форматирования, как правило, применяется только при изготовлении жесткого диска. Обнаружение попытки выполнить такое действие обычно свидетельствует о наличии нового вируса. Это не всегда справедливо для компьютеров NEC PC98xx.

- Запись в загрузочные секторы жесткого диска: Лишь очень немногие программы записывают данные в загрузочные записи. Обнаружение попытки выполнить такое действие может свидетельствовать о наличии нового вируса.
- Запись в загрузочные секторы гибкого диска: Очень немногие программы (такие, как команда Format операционной системы) записывают данные в загрузочные записи гибких дисков. Обнаружение попытки выполнить такое действие может свидетельствовать о наличии нового вируса.

9 Заблокируйте параметры постоянной защиты клиентов, которые вы планируете передавать клиентам.

10 При настройке параметров постоянной защиты для группы серверов нажмите кнопку **Сбросить**, чтобы быть уверенным в том, что все компьютеры будут использовать конфигурацию постоянной защиты, заданную на этом уровне.

См. «Настройка и сброс параметров постоянной защиты» на стр. 92.

11 Нажмите кнопку OK.

Выбор типов дисков для постоянной защиты

При настройке постоянной защиты для файлов вы можете указать, для каких типов дисков должны выполняться осмотры Symantec AntiVirus Corporate Edition:

- Дискеты (только Windows 3.1): Symantec AntiVirus Corporate Edition может проверять файлы при их чтении или записи на дискеты. Дискеты часто становятся источником заражения, поскольку пользователи могут принести зараженные диски из дома.
- Компакт-диски (только Windows 3.1): Иногда случается, что производители программного обеспечения распространяют компакт-диски с зараженными файлами.
- Сетевые диски: Если включена постоянная защита сетевых дисков, то Symantec AntiVirus Corporate Edition может проверять файлы при их записи с компьютера-клиента на сервер (или с одного сервера на другой). Эта возможность является излишней, если включена постоянная защита на серверах. Например, если вы включили постоянную защиту сетевых дисков на клиенте A и на сервере B, то при записи клиентом A файла на сетевой диск сервера B Symantec AntiVirus Corporate Edition сначала осмотрит файл на клиенте A, а затем на сервере B, что может привести к снижению производительности при работе с сетью на клиентском компьютере.

Настройка дополнительных параметров постоянной защиты файловой системы

Существует три параметра постоянной защиты файловой системы, определяющих отслеживаемые операции. Список и описание этих параметров приведены в Табл. 3-2.

Табл. 3-2 Дополнительные параметры постоянной защиты файловой системы

Параметр	**Описание**	**Рекомендации по использованию**
Изменение (осмотр при создании)	Осмотр файлов при их записи, изменении и копировании.	Этот параметр позволяет несколько повысить производительность, поскольку функция постоянной защиты проверяет файлы лишь при их записи, изменении и копировании.
Обращение или изменение (осмотр при создании, открытии. перемещении, копировании или запуске)	Осмотр файлов при их записи, открытии, перемещении, копировании и запуске.	Данный параметр обеспечивает более надежную защиту системы. Обратите внимание, что выбор этого значения может привести к снижению производительности, поскольку функция постоянной защиты проверяет файлы при выполнении любых операций с ними.
Открытие для резервного копирования	На компьютерах, работающих под управлением Windows NT/2000/XP, это значение позволяет проверить файлы, к которым система обращается при резервном копировании.	Этот параметр следует применять, если вы не проверяли наличие вирусов в сохраняемых файлах. Использование данного параметра может существенно замедлить операцию резервного копирования, поскольку функция постоянной защиты будет проверять каждый сохраняемый файл.

Настройка постоянной защиты электронной почты

Функция постоянной защиты может проверять вложения в сообщения электронной почты следующих приложений:

- Lotus Notes 4.5x, 4.6 и 5.0
- Microsoft Exchange 5.0 и 5.5
- Microsoft Outlook 97/98/2000/2002 (только MAPI, не Интернет)

Symantec AntiVirus Corporate Edition непрерывно проверяет вложения в сообщения электронной почты при получении и передаче данных компьютером. Стандартные средства проверки электронной почты Symantec AntiVirus Corporate Edition проверяют наличие зараженных вложений при открытии сообщения.

Symantec AntiVirus Corporate Edition поддерживает осмотр вложений только для клиентов Symantec AntiVirus Corporate Edition.

Настройка осмотра электронной почты

1. В консоли Symantec System Center щелкните правой кнопкой мыши на настраиваемом сервере или группе серверов и выберите команды **Все задачи** > **Symantec AntiVirus** > **Параметры постоянной защиты клиента**.
2. В окне параметров постоянной защиты клиента на вкладке Lotus Notes или Microsoft Exchange установите флажок **Включить постоянную защиту**.

   Вкладка Microsoft Exchange позволяет настраивать защиту как для Microsoft Exchange, так и для Microsoft Outlook.
3. Настройте параметры постоянной защиты.

   Вы можете:
   - Выбрать файлы для осмотра по типам и по расширениям
   - Назначить первичные и вторичные действия, выполняемые при обнаружении вирусов
   - Включить вывод сообщения на экран зараженных компьютеров
   - Включить вставку уведомления в сообщение электронной почты
   - Отправить сообщение отправителю зараженного вложения
   - При обнаружении вируса разослать сообщение выбранным получателям
4. Для настройки проверки сжатых файлов нажмите кнопку **Дополнительно**.
5. Настройте необходимые параметры и нажмите кнопку **OK**.
6. Заблокируйте или разблокируйте параметры по своему усмотрению.
7. Нажмите кнопку **Сбросить**, чтобы обеспечить применение одинаковых параметров постоянной защиты, настроенных на более высоком уровне.

См. «Настройка постоянной защиты» на стр. 86.

Если ваша программа электронной почты не поддерживается

Если ваша система электронной почты не входит в число поддерживаемых продуктов, то для защиты сети можно включить постоянную защиту файловой системы. Например, если вы работаете с системой электронной почты Novell GroupWise и один из пользователей получает сообщение, содержащее зараженное вложение, то Symantec AntiVirus Corporate Edition сможет обнаружить вирус сразу после того, как пользователь дважды щелкнет на вложенном файле, чтобы открыть его. Это связано с тем, что при запуске пользователем вложенного файла большинство почтовых программ (включая GroupWise) сохраняют вложения во временном каталоге. Если включена постоянная защита файловой системы, то Symantec AntiVirus Corporate Edition обнаружит вирус при записи файла во временный каталог. Кроме того, Symantec AntiVirus Corporate Edition обнаружит вирус при попытке пользователя сохранить зараженное вложение на локальном или сетевом диске.

Настройка исключений

Исключения позволяют соблюдать баланс между уровнем защиты сети и объемом ресурсов и временем, необходимым для обеспечения этой защиты. Например, если проверяются файлы всех типов, то можно исключить определенные папки, которые содержат только данные и не могут заражаться вирусами. Это снижает затраты времени и ресурсов, связанные с проверкой файлов.

Настройка и сброс параметров постоянной защиты

Вы можете устанавливать и сбрасывать параметры постоянной защиты на уровне сервера, группы серверов или группы клиентов. При установке и сбросе параметров постоянной защиты необходимо соблюдать следующие правила:

- Изменение параметров постоянной защиты для отдельного сервера позволяет передавать на этот сервер нужную конфигурацию, переопределяя параметры, заданные на уровне группы серверов. Сброс параметров постоянной защиты сервера на уровне группы серверов позволяет сбросить предыдущие параметры, заданные на уровне отдельного сервера.
- Изменение параметров постоянной защиты клиента на уровне родительского сервера или группы клиентов позволяет передавать

нужную конфигурацию клиентам этого родительского сервера или группы клиентов.

- Сброс параметров постоянной защиты клиента на уровне группы серверов позволяет сбросить предыдущие параметры, заданные для всех клиентов на уровне родительского сервера или группы клиентов.
- Изменение параметров постоянной защиты клиента на уровне родительского сервера приводит к изменению параметров для клиентов, не входящих в группы клиентов; клиенты, входящие в группы клиентов, сохраняют свою настройку.

- Нажатие кнопки OK в окне параметров постоянной защиты приводит к заданию лишь тех параметров, которые вы просмотрели или изменили при работе с окном диалога. Неизмененные и непросмотренные параметры не настраиваются. Допустим, например, что при настройке постоянной защиты клиентов вы выполнили следующие действия:
    - Изменили параметры постоянной защиты файловой системы, но не просматривали и не изменяли параметры, указанные на других вкладках или в других окнах диалога.
    - Нажали **OK**.
    - Будут изменены только параметры постоянной защиты файловой системы.
- Нажатие кнопки «Сбросить все» приводит к сбросу всех параметров, настраиваемых с помощью этого окна диалога, независимо от того, просматривали вы их или нет.

Настройка и сброс параметров постоянной защиты

1. С помощью Symantec System Center выполните одно из следующих действий:
    - Для изменения параметров постоянной защиты сервера щелкните правой кнопкой мыши на сервере или группе серверов, и выберите команды **Все задачи** > **Symantec AntiVirus** > **Параметры постоянной защиты сервера**.
    - Для изменения параметров постоянной защиты клиента щелкните правой кнопкой мыши на сервере, группе серверов или группе клиентов, и выберите команды **Все задачи** > **Symantec AntiVirus** > **Параметры постоянной защиты клиента**.
2. В окне параметров постоянной защиты измените нужные параметры.
3. Нажимайте **OK** до возврата к главному окну Symantec System Center.

Блокировка и разблокирование параметров постоянной защиты

Значки замка в окне параметров постоянной защиты позволяют указать, может ли пользователь клиента Symantec AntiVirus Corporate Edition работать с различными параметрами. В Табл. 3-3 приведены возможные значки и их описания.

Табл. 3-3 Блокировка и разблокирование параметров постоянной защиты

Значок	Описание	Значение
	Параметр не заблокирован.	Пользователи могут изменять разблокированные параметры с клиента Symantec AntiVirus Corporate Edition.
	Параметр заблокирован.	Данный параметр недоступен пользователям клиента Symantec AntiVirus Corporate Edition.

Настройка ручных осмотров

Для настройки ручных осмотров необходимо выполнить следующие задачи:

- Выбрать сервер или клиента Symantec AntiVirus Corporate Edition
- Выбрать папки для осмотра
- Задать параметры осмотра
- Задать дополнительные параметры

Примечание: Для осмотра всех серверов и клиентов в группе серверов запустите сплошную проверку или создайте плановый осмотр.

Настройка ручного осмотра

1 С помощью консоли Symantec System Center выполните одно из следующих действий.
   - Щелкните правой кнопкой мыши на сервере или клиенте
   - Выберите один или несколько серверов, входящих в одну группу серверов, и щелкните на них правой кнопкой мыши

- Выберите один или несколько клиентов, управляемых одним сервером, и щелкните на них правой кнопкой мыши

2 Выберите команды **Все задачи** > **Symantec AntiVirus** > **Начать ручной осмотр**.

3 В окне выбора объектов выберите папки для осмотра.

Если проводится осмотр нескольких компьютеров, то такая возможность отсутствует. Переходите к шагу 5.

4 Для того чтобы Symantec AntiVirus Corporate Edition сохранил выбранную настройку ручных осмотров на локальном компьютере, нажмите кнопку **Сохранить**.

Эти настройки будут сохранены Symantec AntiVirus Corporate Edition для последующих осмотров и в том случае, если выбрано несколько компьютеров.

5 Нажмите кнопку **Параметры**.

6 В окне параметров осмотра вы можете выполнить следующие действия:

- Выбрать файлы для осмотра по типам и по расширениям
- Включить вывод сообщения на экран зараженных компьютеров
- Исключить файлы и папки из числа подлежащих осмотру (при выборе нескольких клиентов или серверов этот параметр недоступен)
- Настроить использование ресурсов процессора
- Назначить первичные и вторичные действия, выполняемые при обнаружении вирусов

7 Нажмите кнопку **Дополнительно**.

8 В окне дополнительных параметров осмотра вы можете выполнить следующие действия:

- Указать, нужно ли проверять сжатые файлы. Если проверка включена, можно задать уровень распаковки вложенных архивов. По умолчанию задана проверка до 3 уровней вложенности.
- Включить создание резервных копий файлов перед попыткой их исправления, чтобы предотвратить возможную потерю данных. Файлы будут зашифрованы и помещены в специальную папку в изоляторе. После создания резервной копии файла для доступа к нему необходимо восстановить этот файл.
- Указать, следует ли показывать индикатор выполнения осмотра на экране проверяемого компьютера. Можно сделать так, чтобы окно

индикатора автоматически закрывалось после завершения осмотра. Имеется также возможность показать или скрыть кнопку «Стоп» на удаленном компьютере. Если эта кнопка скрыта, то осмотр нельзя остановить с проверяемого компьютера.

- Включить проверку сжатых файлов на серверах NetWare.

9 Для сохранения значений дополнительных параметров нажмите кнопку **OK**.

10 В окне параметров осмотра нажмите кнопку **Сохранить**, чтобы Symantec AntiVirus Corporate Edition запомнил выбранные значения для последующих ручных осмотров на этом компьютере.

Эти настройки будут сохранены Symantec AntiVirus Corporate Edition для последующих осмотров и в том случае, если выбрано несколько компьютеров.

11 Нажмите кнопку **OK**, чтобы продолжить работу с выбранными значениями.

12 Нажмите кнопку **Пуск**.

См. «Настройка уровня использования ресурсов процессора» на стр. 128.

Настройка плановых осмотров

Для настройки плановых осмотров необходимо выполнить следующие задачи:

- Планирование осмотров для серверов и клиентов Symantec AntiVirus Corporate Edition.
- Настройка обработки пропущенных плановых осмотров.
- Дополнительное изменение, удаление или отключение осмотра, а также запуск планового осмотра по запросу.

Параметры плановых осмотров аналогичны параметрам осмотров постоянной защиты, однако каждый тип осмотра настраивается отдельно. Например, исключения, заданные для функции постоянной защиты, относятся только к этой функции и не влияют на плановые осмотры.

Планирование осмотров для групп серверов и отдельных серверов Symantec AntiVirus Corporate Edition

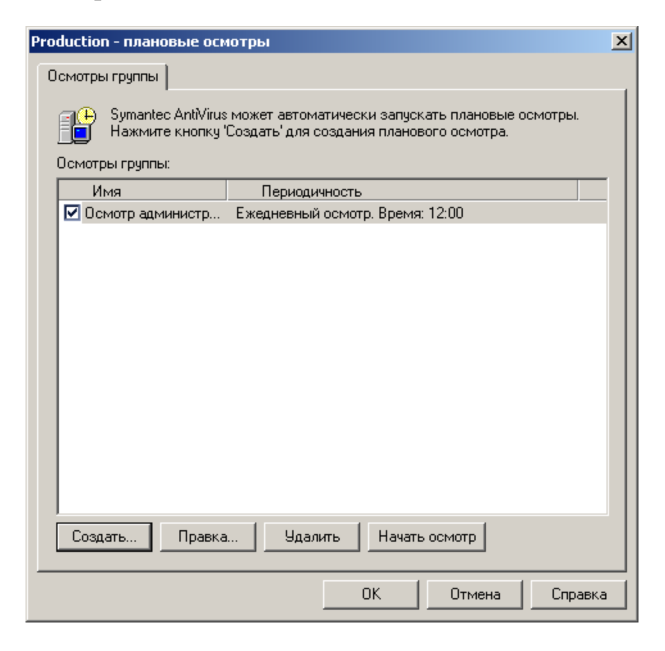
Вы можете настроить плановые осмотры для одной или нескольких групп серверов, а также для отдельных серверов Symantec AntiVirus Corporate Edition.

Планирование осмотра для группы серверов

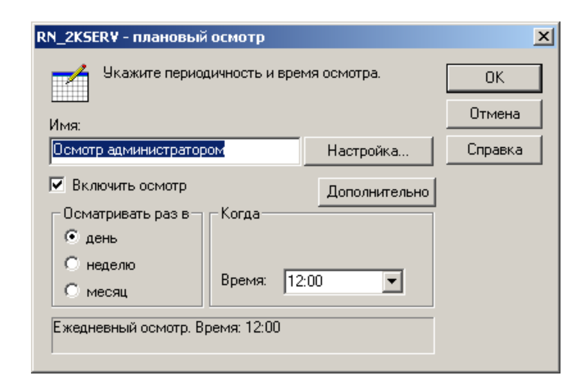
1 С помощью консоли Symantec System Center выполните одно из следующих действий:

- В окне консоли щелкните на структуре системы. С помощью сочетаний Shift+щелчок или Ctrl+щелчок выделите несколько групп серверов, а затем щелкните правой кнопкой мыши на выделенных объектах.
- Щелкните на группе серверов правой кнопкой мыши.
- Щелкните на сервере правой кнопкой мыши.

2 Выберите команды **Все задачи** > **Symantec AntiVirus** > **Плановые осмотры.**



3 В окне плановых осмотров на вкладке «Осмотры сервера» нажмите кнопку **Создать**.



4 В окне плановых осмотров введите название осмотра.

5 Задайте частоту осмотра.

6 Задайте время запуска осмотра.

Можно указать любое время с шагом в 1 минуту или воспользоваться списком, чтобы выбрать время с шагом в 15 минут.

7 Нажмите кнопку **Дополнительно**.

8 На вкладке дополнительных параметров осмотра установите флажок **Обрабатывать пропущенные события не позднее** и задайте промежуток времени, в течение которого будет возможен запуск пропущенной операции.

Например, можно разрешить запуск еженедельного осмотра в течение трех дней после момента времени, заданного для выполнения этой операции.

9 Нажмите кнопку **OK**.

10 В окне плановых осмотров **Настройка**.

11 В окне выбора объектов нажмите кнопку **Параметры**.

12 В окне параметров планового осмотра вы можете выполнить следующие действия:

- Выбрать файлы для осмотра по типам и по расширениям
- Включить вывод сообщений на экран зараженных компьютеров
- Отключить осмотр файлов с определенными расширениями
- Настроить использование ресурсов процессора

- Назначить первичные и вторичные действия, выполняемые при обнаружении вирусов

13 Нажмите кнопку **Дополнительно**.

14 В окне дополнительных параметров осмотра вы можете выполнить следующие действия:

- Включить отображение индикатора выполнения на проверяемом компьютере
- Включить автоматическое закрытие окна индикатора по окончании осмотра
- Включить создание резервных копий файлов перед попыткой их исправления, чтобы предотвратить возможную потерю данных. Файлы будут зашифрованы и помещены в специальную папку в изоляторе. После создания резервной копии файла для доступа к нему необходимо восстановить этот файл.
- Задать параметры проверки сжатых файлов

15 Нажмите кнопку **OK** столько раз, сколько необходимо, чтобы вернуться в главное окно Symantec System Center.

См. «Настройка параметров осмотра» на стр. 106.

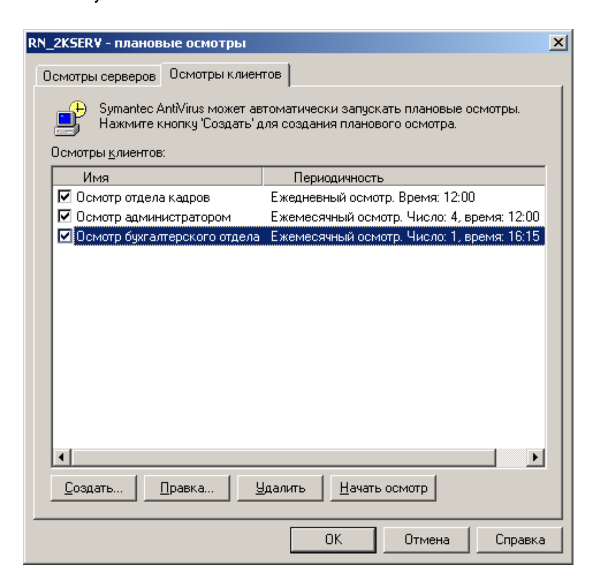
Создание плановых осмотров для клиентов Symantec AntiVirus Corporate Edition

Вы можете запланировать осмотры клиентов Symantec AntiVirus Corporate Edition на уровне сервера или клиента Symantec AntiVirus Corporate Edition.

Создание плановых осмотров для клиентов Symantec AntiVirus Corporate Edition

1 В консоли Symantec System Center щелкните правой кнопкой мыши на сервере или отдельном клиенте, а затем выберите команды **Все задачи** > **Symantec AntiVirus** > **Плановые осмотры**.

2 В окне плановых осмотров на вкладке «Осмотры клиентов» нажмите кнопку **Создать**.



3 В окне плановых осмотров введите название осмотра.

4 Задайте частоту осмотра.

5 Задайте время запуска осмотра.

Можно указать любое время с шагом в 1 минуту или воспользоваться списком, чтобы выбрать время с шагом в 15 минут.

6 Нажмите кнопку **Дополнительно**.

7 На вкладке дополнительных параметров осмотра установите флажок **Обрабатывать пропущенные события не позднее** и задайте промежуток времени, в течение которого будет возможен запуск пропущенной операции.

Например, можно разрешить запуск еженедельного осмотра в течение трех дней после момента времени, заданного для выполнения этой операции.

8 Нажмите кнопку **OK**.

9 В окне плановых осмотров нажмите кнопку **Настройка**.

10 Выберите папки для осмотра. Эта возможность отсутствует при осмотре нескольких компьютеров из-за принадлежности папок к каждому отдельному компьютеру.

11 Нажмите кнопку **Параметры**.

12 В окне параметров планового осмотра вы можете выполнить следующие действия:

- Выбрать файлы для осмотра по типам и по расширениям
- Настроить вывод сообщения на экран зараженного компьютера
- Отключить просмотр отдельных файлов по их расширениям, либо по диску и папке
- Настроить использование ресурсов процессора
- Назначить первичные и вторичные действия, выполняемые при обнаружении вирусов

13 Нажмите кнопку **Дополнительно**.

14 В окне дополнительных параметров осмотра вы можете выполнить следующие действия:

- Включить индикатор выполнения на проверяемом компьютере
- Включить автоматическое закрытие окна индикатора по окончании осмотра
- Включить создание резервных копий файлов перед попыткой их исправления, чтобы предотвратить возможную потерю данных. Файлы будут зашифрованы и помещены в специальную папку в изоляторе. После создания резервной копии файла для доступа к нему необходимо восстановить этот файл.
- Задать параметры проверки сжатых файлов

15 Нажмите кнопку **OK** столько раз, сколько необходимо, чтобы вернуться в главное окно Symantec System Center.

См. «Настройка параметров осмотра» на стр. 106.

Настройка обработки пропущенных плановых осмотров

Если на компьютере не был выполнен плановый осмотр (например, если компьютер был выключен), то Symantec AntiVirus Corporate Edition в течение заданного времени повторит попытку. Если осмотр по-прежнему не удастся запустить, то осмотр выполнен не будет. По умолчанию применяются следующие интервалы времени:

- Ежедневные осмотры: 8 часов
- Еженедельные осмотры: 3 дня
- Ежемесячные осмотры: 11 дней

Вы можете указать интервал времени, на протяжении которого будут предприниматься попытки запуска планового осмотра.

Настройка обработки пропущенных плановых осмотров

1 В Symantec System Center щелкните правой кнопкой мыши на сервере, группе серверов, группе клиентов или на отдельном клиенте Symantec AntiVirus Corporate Edition, а затем выберите команды **Все задачи** > **Symantec AntiVirus** > **Плановые осмотры**.
2 В окне плановых осмотров выберите один из показанных в списке осмотров.
3 Нажмите кнопку **Правка**.
4 В окне плановых осмотров нажмите кнопку **Дополнительно**.
5 В окне дополнительных параметров планового осмотра выберите **Обрабатывать пропущенные события не позднее**.
6 Укажите интервал времени для повторных попыток осмотра.
7 Нажимайте **OK** до возврата к главному окну Symantec System Center.

Изменение, удаление и выключение планового осмотра

Для того чтобы изменить параметры существующего планового осмотра, его можно редактировать. Для того чтобы ранее созданный плановый осмотр не выполнялся, его можно удалить или отключить.

Изменение, удаление и выключение планового осмотра

Вы можете изменять, удалять и выключать плановые осмотры.

Изменение и удаление планового осмотра

1 В консоли Symantec System Center щелкните правой кнопкой мыши на одной или нескольких группах серверов, на сервере или на клиенте, для которого необходимо изменить или удалить плановый осмотр, и выберите команды **Все задачи** > **Symantec AntiVirus**> **Плановые осмотры**.
2 В окне плановых осмотров выберите одно из следующих значений:
   - Осмотры серверов: Позволяет изменить или удалить осмотры для серверов. Если на этапе 1 был выбран клиент, то этот вариант недоступен.

- Осмотры клиентов: Позволяет изменить или удалить осмотры для клиентов. Если на этапе 1 была выбрана группа серверов, то этот вариант недоступен.

3 Выполните одно из следующих действий:

- Выберите существующий осмотр и нажмите кнопку **Правка**. Измените параметры по своему усмотрению и нажмите кнопку **OK** столько раз, сколько необходимо для возврата в главное окно Symantec System Center.
- Выберите существующий осмотр и нажмите кнопку **Удалить**. Нажмите кнопку **OK** столько раз, сколько необходимо для возврата в главное окно Symantec System Center.

Выключение планового осмотра

1 В консоли Symantec System Center щелкните правой кнопкой мыши на одной или нескольких группах серверов, на сервере или на клиенте, для которого необходимо выключить плановый осмотр, и выберите команды **Все задачи** > **Symantec AntiVirus** > **Плановые осмотры**.

Осмотры, которые можно выключить, зависят от выбранного объекта.

2 В окне плановых осмотров выберите одно из следующих значений:

- Осмотры серверов: Позволяет выключить осмотры для серверов. Если на этапе 1 был выбран клиент, то этот вариант недоступен.
- Осмотры клиентов: Позволяет выключить осмотры для клиентов. Если на этапе 1 была выбрана группа серверов, то этот вариант недоступен.

3 Снимите флажок рядом с созданным ранее осмотром.

4 Нажмите кнопку **OK**.

Запуск планового осмотра по требованию

Когда вы создаете и сохраняете плановый осмотр, Symantec AntiVirus Corporate Edition запоминает, для какой группы серверов, сервера или компьютера создан этот осмотр, а также сохраняет параметры, выбранные вами для этого осмотра.

После настройки планового осмотра (и всех его параметров) вы при необходимости можете запустить этот осмотр в любой момент времени, не запланированный заранее. Так можно сэкономить время, которое пришлось бы затратить на создание ручного осмотра с такими же параметрами.

Запуск планового осмотра по требованию

1 В консоли Symantec System Center щелкните правой кнопкой мыши на группе серверов или на отдельном сервере, и выберите команды **Все задачи** > **Symantec AntiVirus** > **Плановые осмотры**.

2 В окне плановых осмотров выберите одно из следующих значений:

- Осмотры серверов: Позволяет запустить плановый осмотр сервера. Если на этапе 1 была выбрана группа серверов, то этот вариант недоступен.
- Осмотры клиентов: Позволяет запустить плановый осмотр клиента. Если на этапе 1 была выбрана группа серверов, то этот вариант недоступен.

3 Выберите существующий плановый осмотр.

4 Нажмите кнопку **Начать осмотр**.

Управление клиентами Symantec AntiVirus Corporate Edition без постоянного соединения

На каждом сервере Symantec AntiVirus Corporate Edition хранится список клиентов Symantec AntiVirus Corporate Edition, которыми он управляет. Сервер передает этот список Symantec System Center. По умолчанию клиенты подключаются к своим родительским серверам один раз в час, а родительские серверы также один раз в час проверяют списки своих клиентов. Родительские серверы контролируют моменты подключения клиентов и, если клиент не подключается к родительскому серверу более тридцати дней, то сервер удаляет этого клиента из своих списков и заносит в журнал запись об удалении клиента. Когда консоль Symantec System Center в очередной раз запросит у родительского сервера список клиентов, то данный клиент не будет указан в списке.

Вы можете управлять этим процессом, изменяя следующие параметры:

- Интервал хранения сведений о клиенте
- Интервал между сеансами связи клиент-сервер

Управление клиентами Symantec AntiVirus Corporate Edition без постоянного соединения

По умолчанию контрольные сеансы связи клиент-сервер проводятся с интервалом в 60 минут. Этот интервал можно изменить с помощью параметра реестра CheckConfigMinutes.

Интервал хранения данных о клиенте должен быть больше интервала между сеансами связи, поскольку в противном случае родительский сервер будет постоянно удалять и добавлять клиентов.

Если данные о новой конфигурации клиента не будут получены родительским сервером или клиентом сразу, то эта информация будет обновлена в ходе следующего контрольного сеанса связи клиента с сервером.

Изменение интервала хранения информации о клиенте

1. Найдите на родительском сервере следующий ключ реестра:
   HKEY_LOCAL_MACHINE\Software\Intel\LANDesk\VirusProtect6\CurrentVersion
2. В меню «Правка» выберите команды **Создать** > **Параметр DWORD**.
3. Присвойте параметру следующее имя:
   ClientExpirationTimeout
4. Щелкните правой кнопкой мыши на новом параметре и выберите команду **Изменить.**
5. В поле значения замените 0 на любое положительное значение.
   Если параметр ClientExpirationTimeout не указан, то по умолчанию используется значение 720 часов. Используйте меньшее значение, чтобы сократить время до удаления клиента из списка консоли, или большее значение, чтобы увеличить это время. Например, если многие компьютеры-клиенты удаляются из списка консоли в связи с тем, что во время отсутствия сотрудников в офисе их компьютеры были выключены, то можно указать большее значение.
6. Нажмите кнопку **OK**.
7. Закройте программу Regedit.

Изменение интервала между сеансами связи клиент-сервер

1. В консоли Symantec System Center щелкните правой кнопкой мыши на группе серверов, группе клиентов или отдельном сервере, и выберите команды **Все задачи** > **Symantec AntiVirus** > **Диспетчер описаний вирусов**.

2 В окне диспетчера описаний вирусов выберите команду **Обновлять описания с родительского сервера**.

3 Нажмите кнопку **Настройка**.

4 В окне настройки обновления укажите в поле «Проверять наличие обновлений каждые» интервал обновления в минутах.

5 Нажимайте **OK** до возврата к главному окну Symantec System Center.

Настройка параметров осмотра

Большинство параметров можно настроить для осмотров разных типов. Например, первичные и вторичные действия можно выбрать как при настройке постоянной защиты, так и при настройке ручного или планового осмотра.

Назначение первичных и вторичных действий, выполняемых при обнаружении вирусов

Вы можете указать первичное действие, которое должно выполняться продуктом Symantec AntiVirus Corporate Edition при обнаружении вирусов, а также вторичное действие, которое следует предпринимать в том случае, если первичное действие выполнить невозможно. Можно выбрать разные действия для применения к макровирусам и к прочим вирусам.

При обнаружении вирусов могут выполнять следующие действия:

- Удалить вирус из файла: Предпринимается попытка исправить зараженный файл при обнаружении вируса.
- Изолировать файл: Сразу после обнаружения вируса предпринимается попытка переместить зараженный файл в изолятор на зараженном компьютере. После того как зараженный файл перемещен в изолятор, ни один пользователь не сможет запустить его, пока не будет предпринято действие (например, исправление или удаление) и файл не будет перемещен в исходную папку.
- Удалить зараженный файл: Предпринимается попытка удалить зараженный файл. Применяйте это действие только в том случае, если имеется возможность заменить удаляемый файл не зараженной резервной копией, поскольку файл удаляется без возможности восстановления с помощью Корзины.
- Не исправлять: Доступ к файлу запрещается, показывается уведомление о наличии вируса и создается запись журнала. Этот

вариант позволит вам выбрать способ обработки вируса. При получении уведомления о заражении вы можете открыть Журнал вирусов для этого компьютера, щелкнуть правой кнопкой мыши на имени зараженного файла и выбрать одно из следующих действий: «Исправить», «Удалить» или «Изолировать».

По умолчанию Symantec AntiVirus Corporate Edition сначала пытается исправить файл. Если Symantec AntiVirus Corporate Edition не удается исправить файл, то файл перемещается в изолятор на зараженном компьютере, доступ к файлу запрещается, а в журнал событий заносится соответствующее сообщение.

Управление доступом пользователей

Symantec AntiVirus Corporate Edition позволяет управлять доступом пользователей клиентов Symantec AntiVirus Corporate Edition к различным параметрам и функциям продукта. Вы можете задавать следующие настройки:

- Разрешать или запрещать пользователям выгрузку Symantec AntiVirus Corporate Edition
- Запрашивать пароль перед разрешением удаления
- Разрешать пользователям приостановку или завершение планового осмотра
- Показывать окно индикатора выполнения
- Настраивать вывод сообщения на экран зараженного компьютера
- Добавлять предупреждение в зараженное сообщение электронной почты
- Уведомлять отправителя зараженного сообщения электронной почты
- Уведомлять других пользователей о получении зараженного сообщения электронной почты

Разрешение и запрет выгрузки Symantec AntiVirus Corporate Edition пользователями

Вы можете разрешить или запретить пользователям выгрузку Symantec AntiVirus Corporate Edition.

Разрешение и запрет выгрузки Symantec AntiVirus Corporate Edition пользователями

1. В консоли Symantec System Center щелкните правой кнопкой мыши на группе серверов, группе клиентов или отдельном сервере, и выберите команды **Все задачи** > **Symantec AntiVirus** > **Параметры клиента (только для администратора)**.
2. Откройте вкладку «Безопасность».
3. Измените значение параметра **Блокировать возможность выгрузки Symantec AntiVirus Services пользователями**.
4. Нажмите кнопку **OK**.

Запрос пароля перед удалением

Вы можете потребовать от пользователя ввода пароля перед удалением Symantec AntiVirus Corporate Edition.

Запрос пароля перед удалением

1. В консоли Symantec System Center щелкните правой кнопкой мыши на группе серверов, группе клиентов или отдельном сервере, и выберите команды **Все задачи** > **Symantec AntiVirus** > **Параметры клиента (только для администратора)**.
2. Откройте вкладку «Безопасность».
3. Установите флажок **Запрашивать пароль для разрешения удаления клиента Symantec AntiVirus.**
4. Нажмите кнопку **Изменить.**
5. В окне изменения пароля введите новый пароль и подтвердите его.
6. Нажимайте **OK** до возврата к главному окну Symantec System Center.

Разрешение приостановки и завершения планового осмотра пользователями

Вы можете разрешить пользователям приостанавливать или откладывать плановый осмотр, а также совсем завершать его. Результаты этих действий:

- Приостановленный осмотр: Когда пользователь приостанавливает осмотр, окно результатов осмотра остается открытым, ожидая, пока пользователь возобновит или прервет осмотр. При выключении компьютера приостановленный осмотр не продолжается.

- Отложенный осмотр: Когда пользователь откладывает плановый осмотр, то, в зависимости от конфигурации, этот осмотр может быть отложен на один час или на три часа. Кроме того, вы можете указать, сколько раз можно отложить осмотр. Если осмотр отложен, то окно результатов осмотра закрывается и появляется вновь после истечения заданного интервала времени и возобновления осмотра.

Разрешение приостановки, откладывания и завершения осмотра

Приостановленный осмотр можно автоматически запустить после истечения определенного интервала времени. Остановленный осмотр не запускается повторно.

Разрешение приостанавливать или откладывать осмотр

1. В Symantec System Center щелкните правой кнопкой мыши на сервере, группе серверов или группе клиентов, и выберите команды **Все задачи** > **Symantec AntiVirus** > **Плановые осмотры**.
2. В окне плановых осмотров выполните одно из следующих действий:
   - Выберите существующий осмотр и нажмите кнопку **Правка**
   - Нажмите кнопку **Создать**, чтобы создать новый осмотр
3. В окне плановых осмотров нажмите кнопку **Настройка**.
4. В окне выбора объектов нажмите кнопку **Параметры**.
5. В окне плановых осмотров нажмите кнопку **Дополнительно**.
6. В окне дополнительных параметров осмотра установите флажок **Индикатор выполнения на проверяемом компьютере**.
7. Снимите флажок **Разрешить пользователю остановку осмотра**.
8. Установите флажок **Разрешить пользователю приостановку/откладывание осмотра**.
9. Нажмите кнопку **Параметры приостановки осмотра**.
10. В окне параметров приостановки выполните одно из следующих действий:
    - Ограничьте максимальное время, на которое пользователь может приостановить осмотр: Установите флажок **Ограничить время приостановки осмотра** и укажите время в минутах.
    - Ограничьте количество приостановок осмотра пользователем: Укажите число в поле **Сколько раз осмотр можно отложить**.

- Включите кнопку осмотра, отложенного на три часа: Установите флажок **Включить кнопку «Отложить осмотр на 3 часа».**

11 Нажимайте **OK** до возврата к главному окну Symantec System Center.

Разрешение завершения осмотра

1 В Symantec System Center щелкните правой кнопкой мыши на сервере, группе серверов или группе клиентов, и выберите команды **Все задачи** > **Symantec AntiVirus** > **Плановые осмотры**.

2 В окне плановых осмотров выполните одно из следующих действий:

- Выберите существующий осмотр и нажмите кнопку **Правка**.
- Нажмите кнопку **Создать**, чтобы создать новый осмотр.

3 В окне плановых осмотров нажмите кнопку **Настройка**.

4 В окне выбора объектов нажмите кнопку **Параметры**.

5 В окне плановых осмотров нажмите кнопку **Дополнительно**.

6 В окне дополнительных параметров осмотра установите флажок **Индикатор выполнения на проверяемом компьютере**.

7 Установите флажок **Разрешить пользователю остановку осмотра**.

8 Снимите флажок **Разрешить пользователю приостановку/откладывание осмотра**.

9 Если вы хотите, чтобы индикатор выполнения осмотра автоматически закрывался после завершения осмотра, установите флажок **Закрыть окно индикатгора по окончании осмотра**.

10 Нажимайте **OK** до возврата к главному окну Symantec System Center.

Настройка и вывод сообщения на экран зараженного компьютера

При выполнении дистанционного осмотра компьютера-клиента имеется возможность немедленно уведомить пользователя о возникших проблемах путем отображения сообщения на экране зараженного компьютера. Можно настроить сообщение об обнаружении вируса таким образом, чтобы оно содержало информацию о названии вируса, имени и состоянии зараженного файла и т. д.

Стандартное сообщение содержит поля переменных и текст. Переменные заключаются в квадратные скобки. Вся информация, не заключенная в скобки, является текстом. Вы можете изменять текст сообщения и

включенные в него переменные по своему усмотрению. Табл. 3-4 содержит описание переменных сообщения.

Табл. 3-4 Переменные сообщений

Переменная	Текст
[LoggedBy]	Тип осмотра, который зарегистрировал событие: постоянная защита, ручной или плановый осмотр.
[Event]	Тип события, например, «Обнаружен вирус».
[VirusName]	Имя обнаруженного вируса.
[PathAndFilename]	Полный путь и имя файла.
[Location]	Путь к диску на зараженном компьютере.
[Computer]	Имя компьютера.
[User]	Сетевое имя зарегистрированного пользователя.
[ActionTaken]	Примененное к зараженному файлу действие (например, исправлен, перемещен в изолятор, удален или не исправлен).
[DateFound]	Дата и время обнаружения вируса.
[Status]	Состояние файла: «Заражен», «Не заражен» или «Удален». Эта переменная не используется по умолчанию. Для того чтобы сообщение содержало это информацию, необходимо вручную добавить переменную в сообщение.

Например, сообщение об обнаружении вируса может выглядеть следующим образом:

```
Тип осмотра: Плановый осмотр
Событие: Обнаружен вирус
Имя вируса: Stoned-C
Файл: C:\Autoexec.bat
Расположение: C:
Компьютер: ACCTG-2
Пользователь: JSmith
Действие: Исправлен
```

Настройка и вывод сообщения на экран зараженного компьютера

1. В консоли Symantec System Center щелкните правой кнопкой мыши на группе серверов, группе клиентов или отдельном сервере Symantec AntiVirus Corporate Edition, и выберите команды **Все задачи** > **Symantec AntiVirus** > **Параметры постоянной защиты клиента**.
2. В окне параметров постоянной защиты клиента установите флажок **Выводить сообщение на зараженный компьютер**.
3. Выполните одно из следующих действий:
   - Примите сообщение по умолчанию, нажав кнопку **OK**
   - Нажмите кнопку **Сообщение**, настройте собственный текст сообщения, и нажмите **OK**
4. Нажимайте кнопку **OK** до возврата к окну параметров постоянной защиты клиента.

Добавление предупреждения в зараженное сообщение электронной почты

Вы можете настроить постоянную защиту таким образом, чтобы в текст зараженных сообщений электронной почты, обрабатываемых поддерживаемыми программами, автоматически добавлялись предупреждения. Этот тип оповещения может оказаться полезным в случае, если Symantec AntiVirus Corporate Edition не может исправить зараженное сообщение, и файл вложения перемещен, оставлен без изменения, удален или переименован. Предупреждающее сообщение содержит информацию об обнаруженном вирусе и предпринятом действии.

Symantec AntiVirus Corporate Edition добавляет в начало почтового сообщения, содержащего зараженное вложение, следующий текст:

Symantec AntiVirus Corporate Edition обнаружил вирус во вложении от [Отправитель почтового сообщения].

Для каждого зараженного файла в сообщение также добавляется следующая информация:

- Имя вложенного файла
- Название обнаруженного вируса
- Предпринятое действие (например, исправлен, перемещен в изолятор, удален или не исправлен)
- Состояние файла (заражен или не заражен)

Вы можете настраивать тему и текст сообщения.

Это почтовое сообщение содержит поле [EmailSender]. Все поля, заключенные в скобки, служат для представления переменной информации. Вы можете настроить стандартное сообщение, щелкнув правой кнопкой мыши на тексте сообщения и выбрав поле для вставки в сообщение.

Сообщение, полученное пользователем, будет выглядеть следующим образом:

Symantec AntiVirus Corporate Edition обнаружил вирус во вложении от John.Smith@mycompany.com.

Добавление предупреждения в зараженное сообщение электронной почты

1. В консоли Symantec System Center щелкните правой кнопкой мыши на группе серверов, группе клиентов или отдельном сервере Symantec AntiVirus Corporate Edition, и выберите команды **Все задачи** > **Symantec AntiVirus** > **Параметры постоянной защиты клиента**.
2. В окне параметров постоянной защиты клиента на вкладке Lotus Notes или Microsoft Exchange установите флажок **Вставлять уведомления в сообщения электронной почты**.
3. Выполните одно из следующих действий:
   - Примите сообщение по умолчанию, нажав кнопку **OK**
   - Нажмите кнопку **Предупреждение**, настройте собственный текст сообщения, и нажмите **OK**
4. Нажимайте кнопку **OK** до возврата к окну параметров постоянной защиты клиента.

Уведомление отправителя зараженного сообщения электронной почты

При работе с поддерживаемыми программами электронной почты вы можете настроить постоянную защиту таким образом, чтобы отправителю сообщения с зараженным вложением отправлялось уведомление.

Symantec AntiVirus Corporate Edition отправляет ответное сообщение со следующей темой:

В сообщении «[Тема почтового сообщения]» обнаружен вирус.

В тексте сообщения, отправляемого отправителю, указывается информация о зараженном вложении:

Symantec AntiVirus Corporate Edition обнаружил вирус во вложении, отправленном вами ([Отправитель почтового сообщения]) по адресу [Список получателей сообщения].

Для каждого зараженного файла в сообщение также добавляется следующая информация:

- Имя вложенного файла
- Название обнаруженного вируса
- Предпринятое действие (например, исправлен, перемещен в изолятор, удален или не исправлен)
- Состояние файла (заражен или не заражен)

Уведомление отправителя зараженного сообщения электронной почты

1. В консоли Symantec System Center щелкните правой кнопкой мыши на группе серверов, группе клиентов или отдельном сервере Symantec AntiVirus Corporate Edition, и выберите команды **Все задачи** > **Symantec AntiVirus** > **Параметры постоянной защиты клиента**.
2. В окне параметров постоянной защиты клиента на вкладке Lotus Notes или Microsoft Exchange установите флажок **Включить постоянную защиту Lotus Notes** (**Microsoft Exchange**).
3. Установите флажок **Отправить сообщение отправителю**.
4. Нажмите кнопку **Сообщение**.
5. Выполните одно из следующих действий:
   - Примите сообщение по умолчанию, нажав кнопку **OK**
   - Нажмите кнопку **Сообщение**, настройте собственный текст сообщения, и нажмите **OK**
6. Нажимайте кнопку **OK** до возврата к окну параметров постоянной защиты клиента.

Уведомление других пользователей о зараженном сообщении электронной почты

При работе с поддерживаемыми программами электронной почты вы можете настроить постоянную защиту таким образом, чтобы другим

пользователям отправлялось предупреждение о сообщении с зараженным вложением.

Symantec AntiVirus Corporate Edition отправляет выбранным пользователям сообщение со следующей темой:

В сообщении «[Тема почтового сообщения]» обнаружен вирус.

В тексте сообщения указывается информация об отправителе зараженного вложения:

Symantec AntiVirus Corporate Edition обнаружил вирус во вложении от [Отправитель почтового сообщения].

Для каждого зараженного файла в сообщение также добавляется следующая информация:

- Имя вложенного файла
- Название обнаруженного вируса
- Предпринятое действие (например, исправлен, перемещен в изолятор, удален или не исправлен)
- Состояние файла (заражен или не заражен)

Уведомление других пользователей о зараженном сообщении электронной почты

1. В консоли Symantec System Center щелкните правой кнопкой мыши на группе серверов, группе клиентов или отдельном сервере Symantec AntiVirus Corporate Edition, и выберите команды **Все задачи** > **Symantec AntiVirus** > **Параметры постоянной защиты клиента**.
2. В окне параметров постоянной защиты клиента на вкладке Lotus Notes или Microsoft Exchange установите флажок **Включить постоянную защиту Lotus Notes (Microsoft Exchange)**
3. Установите флажок **Отправить сообщение пользователям**.
4. Нажмите кнопку **Адреса.**
5. В окне адресов электронной почты укажите один или несколько адресов, по которым необходимо отправлять уведомления.
6. Нажмите кнопку **OK.**
7. Нажмите кнопку **Сообщение**.
8. Выполните одно из следующих действий:
   - Примите сообщение по умолчанию, нажав кнопку **OK**

- Нажмите кнопку **Создать**, сформируйте текст сообщения и нажмите **OK**

9 Нажимайте кнопку **OK** до возврата к окну параметров постоянной защиты клиента.

Исключение файлов из осмотра

Исключения позволяют соблюдать баланс между уровнем защиты сети и объемом ресурсов и временем, необходимым для обеспечения этой защиты. Например, если проверяются файлы всех типов, то можно исключить определенные папки, которые содержат только данные и не могут заражаться вирусами. Это снижает затраты времени и ресурсов, связанные с проверкой файлов.

Symantec System Center позволяет исключать из осмотра отдельные папки и файлы с заданными расширениями. Кроме того, некоторые виды осмотров Symantec AntiVirus Corporate Edition позволяют исключать папки с определенными именами (например, вы можете исключить из осмотра папку C:\Temp\Install). Для обеспечения безопасности вы не можете просматривать и исключать отдельные файлы с помощью Symantec System Center. Однако вы можете исключить отдельные файлы с помощью пользовательского интерфейса клиента или сервера Symantec AntiVirus Corporate Edition. Таким образом можно исключить из осмотра файлы, выдающие ложные предупреждения о вирусах. Например, если вы применяете другую антивирусную программу, исправляющую зараженные файлы, и эта программа не полностью удаляет код вируса, то файл может быть безвредным, однако обезвреженный код вируса может привести к регистрации ложного предупреждения Symantec AntiVirus Corporate Edition. Обратитесь в службу технической поддержки Symantec, если вы не уверены, заражен файл или нет. Табл. 3-5 содержит описания исключений.

Табл. 3-5 Исключения по типу объектов

Тип объекта	Доступные исключения
Группа серверов	Осмотры серверов: Расширения файлов и папки с заданными именами.
Сервер	■ Осмотры серверов: Расширения файлов, диски, файлы и папки. ■ Осмотры клиентов: Расширения файлов, диски и папки с заданными именами.
Группы клиентов	Осмотры клиентов: Расширения файлов, диски и папки с заданными именами.

Табл. 3-5 Исключения по типу объектов

Тип объекта	Доступные исключения
Серверы NetWare	Файлы на определенных дисках и в папках с заданными именами; исключение файлов по расширению невозможно.

Настройка исключений

Symantec AntiVirus Corporate Edition может проверять исключения до или после выполнения осмотра:

- Если исключения применяются до начала осмотра, то исключенные объекты вообще не проверяются. Если файл не исключен, то он проверяется.
- Если исключения проверяются после выполнения осмотра, то предоставляется информация только о тех вирусах, которые были обнаружены в не исключенных файлах. Постоянная защита Symantec AntiVirus Corporate Edition не предпринимает никаких действий для исключенных файлов.
- При сплошной проверке, ручной проверке, а также при плановом осмотре и при осмотре функцией постоянной защиты Symantec AntiVirus Corporate Edition не предпринимает никаких действий для исключенных файлов.

Включение и выключение проверки исключений перед осмотром позволяет в ряде случаев повысить производительность. Например:

- Если вы копируете большую папку, которая попадает в список исключений и проверка исключений перед осмотром включена, то процесс копирования не займет много времени, поскольку все содержимое папки будет исключено из осмотра до его выполнения.
- Если копируется большая папка, не попадающая в список исключений, отключение проверки исключений перед осмотром позволит выполнить копирование быстрее.

Настройка исключений

1. В окне параметров осмотра необходимого типа установите флажок **Исключить файлы и папки**.
2. Нажмите кнопку **Исключения**.

3 В окне исключений установите флажок **Проверять перед осмотром, не исключен ли файл**, чтобы включить проверку исключений перед осмотром.

4 В зависимости от типов и числа настраиваемых компьютеров, вы можете выполнить следующие действия:

- Выбрать исключаемые файлы с помощью расширения или символов подстановки
- Выбрать исключаемые файлы по их расположению в определенных папках с помощью расширений, типов файлов и символов подстановки
- Выбрать папки для исключения из осмотра

5 Нажимайте **OK** до возврата к консоли Symantec System Center.

Выбор типов и расширений файлов для осмотра

По умолчанию Symantec AntiVirus Corporate Edition проверяет при осмотре все файлы. Для осмотров, выполняемых не функцией постоянной защиты, вы можете включить осмотр только файлов определенного типа или только файлов с определенными расширениями. Осмотр файлов по типу или расширению возможен при выборе следующих объектов и типов осмотра:

- Объект клиента: Ручной осмотр, плановый осмотр и постоянная защита клиента.
- Объект сервера: Сплошная проверка, ручной осмотр и постоянная защита сервера (только для Windows).

При осмотре по типу файлов Symantec AntiVirus Corporate Edition считывает заголовок каждого файла и определяет его тип. Например, если включить осмотр документов, то Symantec AntiVirus Corporate Edition проверит все документы, даже если им были присвоены нестандартные расширения, например, Document3.mlt, а не Document3.doc.

Примечание: Эта функция неприменима к серверам NetWare; она работает только на компьютерах Windows.

При осмотре по расширениям Symantec AntiVirus Corporate Edition не считывает заголовки файлов для определения их типов и проверяет только

файлы с указанными расширениями. В Табл. 3-6 перечислены рекомендуемые расширения.

Табл. 3-6 Расширения файлов, рекомендуемые для осмотра

Расширение файла	Описание
386	Драйвер
ACM	Драйвер; диспетчер сжатия звука
ACV	Драйвер; диспетчер сжатия/распаковки звука
ADT	ADT-файл; факс
AX	AX-файл
BAT	Пакетный файл
BTM	Пакетный файл
BIN	Двоичный файл
CLA	Класс Java
COM	Исполняемый файл
CPL	Аплет панели управления для Microsoft Windows
CSC	Сценарий Corel
DLL	Динамическая библиотека
DOC	Документ Microsoft Word
DOT	Шаблон Microsoft Word
DRV	Драйвер
EXE	Исполняемый файл
HLP	Файл справки
HTA	Приложение HTML
HTM	HTML
HTML	HTML
HTT	HTML
INF	Сценарий установки

Табл. 3-6 Расширения файлов, рекомендуемые для осмотра

Расширение файла	Описание
INI	Файл настройки
JS	JavaScript
JSE	JavaScript с шифром
JTD	Ichitaro
MDB	Файл Microsoft Access
MP?	Файл Microsoft Project
MSO	Файл Microsoft Office 2000
OBD	Подшивка Microsoft Office
OBT	Подшивка Microsoft Office
OCX	Элемент управления Microsoft OLE
OV?	Оверлей
PIF	Файл-описатель программы
PL	Исходный код PERL (UNIX)
PM	Рисунок для диспетчера презентаций
POT	Файл Microsoft PowerPoint
PPT	Файл Microsoft PowerPoint
PPS	Файл Microsoft PowerPoint
RTF	Документ RTF
SCR	Факс, заставка, рисунок, сценарий для Faxview/MS Windows
SH	Сценарий оболочки UNIX
SHB	Файл фона Corel Show
SHS	Файл оболочки
SMM	Файл AmiPro
SYS	Драйвер устройства
VBE	VESA BIOS (функции ядра)

Табл. 3-6 Расширения файлов, рекомендуемые для осмотра

Расширение файла	Описание
VBS	Файл VBScript
VSD	Файл Visio
VSS	Файл Visio
VST	Файл Visio
VXD	Виртуальный драйвер устройства
WSF	Файл сценария Windows
WSH	Файл хост-параметров сценария Windows
XL?	Файл Microsoft Excel

Выбор файлов для осмотра по типам и расширениям

Для всех типов осмотров вы можете выбрать файлы по типу и расширению. Для плановых и ручных осмотров можно также выбрать файлы по типу и расширению на уровне папки.

Выбор файлов для осмотра по расширению

1 В окне параметров осмотра необходимого типа нажмите одну из кнопок **Выбранные**.

2 Нажмите кнопку **Расширения**.

3 В окне выбранных расширений выберите одно из следующих значений:

- Добавить: Позволяет добавить расширение файла, введя его и нажав кнопку **Добавить**.
- Документы: Позволяет добавить все расширения, соответствующие документам.
- Программы: Позволяет добавить все расширения, соответствующие программам.
- По умолчанию: Позволяет добавить все типы программ и расширений.

4 Нажимайте **OK** до возврата к консоли Symantec System Center.

Выбор файлов для осмотра по типу

1. В окне параметров осмотра необходимого типа нажмите одну из кнопок **Выбранные**.
2. Нажмите кнопку **Типы**.
3. В окне выбранных типов выберите одно из следующих значений:
   - Файлы документов: Проверяет файлы документов, независимо от их расширений
   - Файлы программ: Проверяет файлы программ MS DOS и Windows
4. Нажимайте **OK** до возврата к консоли Symantec System Center.

Выбор файлов для ручного осмотра по папкам

1. В окне консоли Symantec System Center щелкните правой кнопкой мыши на объекте для осмотра и выберите команды **Все задачи** > **Symantec AntiVirus** > **Начать ручной осмотр**.
2. В окне выбора объектов выберите папки для осмотра.
3. Нажмите кнопку **Параметры** и выберите расширения и типы файлов для осмотра в выбранных папках.
4. Нажимайте **OK** до возврата к консоли Symantec System Center.

Выбор файлов для планового осмотра по папкам

1. В окне консоли Symantec System Center щелкните правой кнопкой мыши на объекте для осмотра и выберите команды **Все задачи** > **Symantec AntiVirus** > **Плановый осмотр**.
2. На вкладке «Осмотры серверов» выберите осмотр в списке.
3. Нажмите кнопку **Правка**.
4. В окне плановых осмотров нажмите кнопку **Настройка**.
5. В окне выбора объектов выберите папки для осмотра.
6. Нажмите кнопку **Параметры** и выберите расширения и типы файлов для осмотра в выбранных папках.
7. Нажимайте **OK** до возврата к консоли Symantec System Center.

При выборе объекта в иерархической структуре значок изменяется, как показано в Табл. 3-7.

Табл. 3-7 Значки проверки в иерархической структуре

Значок	Описание
	Symantec AntiVirus Corporate Edition будет проверять все находящиеся в этой папке файлы и все файлы, находящиеся во вложенных папках.
	Symantec AntiVirus Corporate Edition будет проверять один или несколько объектов, выбранных в папке или во вложенных папках.
	Symantec AntiVirus Corporate Edition будет проверять выбранный файл. Это значение можно выбрать только с помощью интерфейса клиента или сервера.
	Symantec AntiVirus Corporate Edition не будет проверять эту папку и вложенные папки.

Настройка параметров для проверки сжатых файлов

Табл. 3-8 содержит список и описания параметров осмотра сжатых файлов.

Табл. 3-8 Параметры осмотра сжатых файлов

Операционная система	Параметр осмотра
Windows	Symantec AntiVirus Corporate Edition проверяет сжатые файлы при ручном и плановом осмотре, а также при осмотре электронной почты. Поскольку проверка сжатых файлов, находящихся внутри других сжатых файлов, связана со значительными затратами вычислительных ресурсов, функция постоянной защиты не проверяет такие файлы на компьютерах Windows, однако файлы проверяются при их извлечении из сжатых файлов.
NetWare	Symantec AntiVirus Corporate Edition проверяет сжатые файлы при плановом осмотре, а также при осмотре с помощью функции постоянной защиты. Для осмотра содержимого сжатых файлов Symantec AntiVirus Corporate Edition последовательно извлекает из архива каждый файл, копирует его на том SYS и проверяет. На томе SYS должно быть достаточно свободного пространства для размещения самого большого файла, хранящегося в архиве.

В окне дополнительных параметров осмотра вы можете задать параметры осмотра сжатых файлов, находящихся внутри других сжатых файлов. Если вы установили флажок Проверять содержимое сжатых файлов, то Symantec AntiVirus Corporate Edition будет осматривать сжатые файлы (например, Files.zip) и их содержимое, представляющее собой отдельные сжатые файлы. Symantec AntiVirus Corporate Edition поддерживает до десяти уровней вложенности сжатых файлов; серверы NetWare поддерживают до трех уровней вложенности.

Примечание: Остановить осмотр в ходе проверки сжатого файла нельзя. Если была нажата кнопка «Стоп», то Symantec AntiVirus Corporate Edition остановит осмотр только после завершения проверки текущего сжатого файла.

Настройка HSM

Symantec AntiVirus Corporate Edition включает параметры, позволяющие точно настраивать осмотр файлов, хранящихся в системах иерархического управления памятью (HSM) и в автономных хранилищах резервных копий. Система HSM переносит файлы на дополнительное запоминающее устройство, например, на компакт-диск, на ленту или в хранилище данных SAN, однако часть исходного файла при этом может остаться на диске. Если во время осмотра Symantec AntiVirus Corporate Edition будет обращаться к таким частичным файлам и система HSM при этом будет восстанавливать файлы на исходных дисках, то возможно снижение производительности и возникновение проблем с дисковым пространством. Вы можете обратиться к поставщику HSM или системы резервного копирования и с их помощью выбрать оптимальную настройку. Настройка зависит от алгоритма работы приложения HSM.

Табл. 3-9 содержит список параметров осмотров для HSM в системах Windows 2000 и более поздних версий.

Табл. 3-9 Параметры проверки (Windows 2000 и более поздних версий)

Параметр	Описание
Пропускать автономные файлы	Если установлен бит автономного хранения, то файл пропускается. На установленный бит автономного хранения указывают часы, показанные поверх значка файла в Проводнике. Бит автономного хранения может быть установлен любым приложением, без фактического переноса файла в автономное хранилище.

Табл. 3-9 Параметры проверки (Windows 2000 и более поздних версий)

Параметр	Описание
Пропускать автономные и разреженные файлы	Некоторые приложения устанавливают бит разреженного файла, указывающий, что часть файла отсутствует на диске. Поскольку некоторые продукты HSM устанавливают этот бит, а некоторые нет, то следует обратиться к поставщику системы HSM и узнать, устанавливается ли этот бит в вашем случае. В разреженных файлах небольшая часть файла остается на диске, в то время как большая часть этого файла перемещается в автономное хранилище.
Пропускать автономные и разреженые файлы с точками повторной обработки (объектами Reparse Point)	Некоторые поставщики применяют точки повторной обработки. Приложения, использующие такой подход, применяют также соответствующий драйвер устройства, позволяющий управлять точками повторной обработки в файлах. Это значение по умолчанию в Symantec AntiVirus Corporate Edition, поскольку оно является наиболее надежным для продуктов, применяющих точки повторной обработки. Обратитесь к поставщику системы HSM и узнайте, нужно ли применять это значение. При использовании точек повторной обработки часть файла остается на диске, а прозрачный доступ к остальной части файла обеспечивается с помощью специального фильтра приложения (драйвера устройства).
Осматривать резидентные части автономных и разреженных файлов	Symantec AntiVirus Corporate Edition определяет часть диска, хранящуюся на диске. В разреженных файлах проверяется лишь часть файла, хранящаяся на диске, без обращения к той части, которая находится на дополнительном запоминающем устройстве. Поскольку некоторые производители систем HSM поддерживают такую возможность, а некоторые нет, обратитесь к своему поставщику и узнайте, можно ли применять данное значение.

Табл. 3-9 Параметры проверки (Windows 2000 и более поздних версий)

Параметр	Описание
Осматривать все файлы с выполнением обратной миграции (заполненяет диск)	Файл проверяется полностью; при необходимости он восстанавливается с дополнительного запоминающего устройства. Поскольку объем дополнительного запоминающего устройства как правило больше, чем объем локального тома, выбор этого параметра может привести к заполнению локальных дисков и возникновению сбоев при открытии файлов для осмотра.
Осматривать все файлы без выполнения обратной мигнации (медленно)	Symantec AntiVirus Corporate Edition копирует файл с дополнительного запоминающего устройства на локальный диск в виде временного файла, однако приложение HSM оставляет исходный файл на дополнительном запоминающем устройстве. Этот способ медленный и поддерживается не всеми поставщиками систем HSM. Поскольку для проверки файл копируется с дополнительного запоминающего устройства на диск, возрастают требования к объему ресурсов. Если при проверке будет обнаружен вирус, то при удалении или исправлении файла на дополнительном запоминающем устройстве возможно дальнейшее снижение производительности процессора и сети.
Осматривать все недавно измененные файлы без выполнения обратной миграции	Для сокращения требований к объему ресурсов, предъявляемых при выборе значения «Осматривать все файлы без выполнения обратной миграции», это значение позволяет проверять только файлы, которые были сохранены последними и еще могут находиться на сравнительно быстрых дополнительных запоминающих устройствах. Это значение рекомендуется применять для проверки файлов, все еще хранящихся на сравнительно быстрых дополнительных дисках, не восстанавливая и не проверяя файлы, которые уже перенесены на медленные устройства долговременного хранения. Например, файлы могут переноситься на удаленный диск после 30 дней хранения без обращений. После хранения в течение 60 дней без обращений файл переносится на компакт-диск или в удаленное хранилище данных SAN. Во многих случаях такой способ может быть медленным, поскольку обращение к файлам без их восстановления представляет собой относительно медленную операцию.

Табл. 3-9 Параметры проверки (Windows 2000 и более поздних версий)

Параметр	Описание
Открывать файлы с использованием семантики архивации	Разрешает проверку файлов, чтение которых по соображениям защиты обычно разрешено либо определенному пользователю.

В Табл. 3-10 указан параметр осмотра для HSM в системах NetWare.

Табл. 3-10 Параметры проверки (NetWare)

Параметр	Описание
Осматривать сжатые или мигрируемые файлы NetWare	Проверяются файлы NetWare, сжатые или перенесенные на дополнительное запоминающее устройство.

Настройка параметров HSM

- В окне дополнительных параметров осмотра для осмотра нужного типа выберите требуемые параметры.

Пропуск проверки сохраняемых файлов функцией постоянной защиты

Вы можете указать, что функция постоянной защиты Symantec AntiVirus Corporate Edition должна пропускать проверку файлов во время создания резервной копии. Это позволит программному обеспечению создания резервной копии работать без дополнительных затрат ресурсов, связанных с работой функции постоянной защиты. Данный параметр применяется только к файлам, для которых создается резервная копия. Файлы, восстанавливаемые из резервной копии, проверяются независимо от значения данного параметра.

Примечание: Этот параметр доступен только в системах Windows NT/2000/XP.

Пропуск проверки сохраняемых файлов функцией постоянной защиты

1 В окне параметров постоянной защиты нажмите кнопку **Дополнительно**.

2 В окне дополнительных параметров защиты файловой системы снимите флажок **Открыто для архивации**.

Настройка уровня использования ресурсов процессора

Symantec AntiVirus Corporate Edition позволяет задавать приоритет процесса осмотра для плановых и ручных осмотров. Установка для процесса осмотра низкого приоритета, означает, что процесс осмотра займет больше времени, но при этом предоставит больше ресурсов процессора для выполнения других задач. В некоторых ситуациях целесообразно снизить приоритет. Например, если осмотры выполняются в рабочие дни во время обеденного перерыва, имеет смысл ограничить приоритет, чтобы свести к минимуму влияние осмотра на производительность компьютера.

Задать приоритет процесса осмотра можно с помощью регулятора в окне параметров осмотра. Приоритет процесса осмотра можно задать для следующих систем:

- Компьютеры Windows: Приоритет может задаваться для работающего или простаивающего компьютера. Значение простоя задает приоритет, устанавливаемый для процесса осмотра на простаивающем компьютере. Второе значение задает приоритет, устанавливаемый для процесса осмотра на компьютере, активно выполняющем другие задачи.
- Компьютеры NetWare: Symantec AntiVirus Corporate Edition позволяет настраивать нагрузку на серверы NetWare. Низкое значение нагрузки означает, что осмотр сервера займет больше времени.

Глава 4

Обновление файлов описаний вирусов

Эта глава содержит следующие разделы:

Сведения о файлах описаний вирусов

Файлы описаний вирусов содержат примеры кода тысяч известных вирусов. При осмотре файлов Symantec AntiVirus Corporate Edition пытается найти соответствие между файлами и примерами кода из файлов описаний вирусов. Если Symantec AntiVirus Corporate Edition обнаруживает совпадение, то файл может быть зараженным.

На каждом сервере и клиенте, применяющем Symantec AntiVirus Corporate Edition, хранится копия файлов описаний вирусов. По мере обнаружения новых вирусов эти файлы устаревают. Symantec обновляет файлы описаний вирусов примерно один раз в неделю, а при необходимости и чаще. Для обеспечения максимальной защиты сети важно поддерживать текущий уровень файлов описаний вирусов.

Методы обновления файлов описаний вирусов

Существует четыре метода загрузки описаний вирусов и настройки серверов и клиентов для их получения. В Табл. 4-1 приведены описания методов обновления файлов описаний вирусов.

Табл. 4-1 Методы обновления файлов описаний вирусов

Метод	Описание	Рекомендации по использованию
Метод передачи вирусных описаний	После получения первичным сервером сети новых описаний вирусов с FTP-сайта Symantec или с сервера LiveUpdate запускается операция установки. Первичный сервер передает пакет описаний вирусов на все вторичные серверы в группе серверов. Дополнительные серверы извлекают описания и помещают их в соответствующий каталог. Клиенты получают пакет со своих родительских серверов. Дополнительные серверы извлекают описания и помещают их в соответствующий каталог.	Метод передачи вирусных описаний рекомендуется применять в том случае, когда необходимо управлять обновлением файлов описаний вирусов из Symantec System Center. Кроме того, тот метод может применяться во время эпидемии вирусов для немедленной установки файлов описаний вирусов на компьютеры сети.

Табл. 4-1 Методы обновления файлов описаний вирусов

Метод	Описание	Рекомендации по использованию
Функция LiveUpdate	При запросе новых описаний клиентом или сервером, применяющим LiveUpdate, запускается плановая операция загрузки. Функцию LiveUpdate можно настроить для запроса обновлений с внутреннего сервера LiveUpdate организации или непосредственно с сервера LiveUpdate компании Symantec.	Функцию LiveUpdate рекомендуется применять, когда защищаемые компьютеры должны загружать файл описаний вирусов с внутреннего сервера LiveUpdate или непосредственно с сервера Symantec.
Опрос центрального изолятора	Сервер центрального изолятора периодически опрашивает шлюз Symantec Digital Immune System на предмет наличия новых файлов описаний вирусов. При наличии новых описаний сервер центрального изолятора может автоматически установить эти описания на те компьютеры, которым они необходимы.	Центральный изолятор рекомендуется применять для автоматической рассылки обновленных файлов описаний вирусов в сети.
Программа Intelligent Updater	Intelligent Updater — это самораспаковывающийся исполняемый файл, содержащий файлы описаний вирусов.	Intelligent Updater рекомендуется применять в тех случаях, когда необходимо разослать обновленные файлы описаний вирусов пользователям, не имеющим активного соединения с сетью.

Рекомендуемый метод: Совместное использование метода передачи вирусных описаний и функции LiveUpdate

Вы можете одновременно применять метод передачи вирусных описаний и функцию LiveUpdate. Применение функции LiveUpdate позволяет обновлять компоненты программного обеспечения Symantec AntiVirus Corporate Edition. Применение метода передачи вирусных описаний позволяет планировать и устанавливать обновления файлов описаний вирусов из Symantec System Center. Кроме того, метод передачи вирусных

описаний может применяться в качестве аварийного метода для быстрой рассылки новых файлов описаний вирусов при появлении угрозы заражения сети новым вирусом.

Хотя метод передачи вирусных описаний используется чаще, некоторые крупные сети полагаются на использование функции LiveUpdate. В таких системах не следует разрешать прямой доступ к сайту компании Symantec большому числу серверов и клиентов. Один или несколько серверов выступают в качестве внутренних серверов LiveUpdate для всех остальных серверов сети и, в некоторых случаях, для всех клиентов.

Обновление файлов описаний вирусов на серверах Symantec AntiVirus Corporate Edition

Существует три метода обновления файлов описаний вирусов на серверах:

- Метод передачи вирусных описаний
- Функция LiveUpdate
- Программа Intelligent Updater
- Опрос центрального изолятора

См. «Методы обновления файлов описаний вирусов» на стр. 130.

Обновление и настройка серверов Symantec AntiVirus Corporate Edition с помощью метода передачи вирусных описаний

Ручное обновление серверов Symantec AntiVirus Corporate Edition следует выполнять в том случае, когда требуется немедленное обновление. Плановое автоматическое обновление позволяет обеспечить обычное обновление файлов вирусных описаний, не требующее вмешательства пользователя.

Ручное или автоматическое обновление серверов с помощью метода передачи вирусных описаний

Серверы можно обновлять вручную или автоматически. Обновление выполняется лишь в том случае, если файлы описаний вирусов на сервере более старые, чем определения на сервере LiveUpdate.

Обновление всех разблокированных серверов

1. В окне Symantec System Center щелкните правой кнопкой мыши на структуре системы, и выберите команды **Symantec AntiVirus** > **Обновить описания вирусов...**
2. В окне подтверждения нажмите кнопку **Да**.
3. В окне состояния нажмите **OK**.

Ручное обновление серверов

1. В окне консоли Symantec System Center щелкните правой кнопкой мыши на сервере или группе серверов, и выберите команды **Все задачи** > **Symantec AntiVirus** > **Диспетчер описаний вирусов**.
2. Выберите один из следующих вариантов:
   - Обновлять первичный сервер только этой группы: Позволяет обновить все серверы в группе с первичного сервера.
   - Обновлять каждый сервер в этой группе серверов по отдельности: Позволяет обновлять серверы по отдельности.

   Выбранный параметр относится ко всем серверам группы, независимо от того, выбрали вы группу серверов или отдельный сервер.
3. Нажмите кнопку **Настроить**.
4. Нажмите кнопку **Обновить сейчас**.

   Появится сообщение о том, как увидеть дату выпуска нового файла описаний.
5. Прочтите показанную информацию и нажимайте кнопку **OK** до возврата к консоли Symantec System Center.

Автоматическое обновление серверов

1. В окне Symantec System Center щелкните правой кнопкой мыши на сервере или группе серверов, и выберите команды **Все задачи** > **Symantec AntiVirus** > **Диспетчер описаний вирусов**.
2. Выберите один из следующих вариантов:
   - Обновлять первичный сервер только этой группы: Позволяет автоматически обновить все серверы в группе с первичного сервера.
   - Обновлять каждый сервер в этой группе серверов по отдельности: Позволяет обновлять серверы по отдельности.

   Выбранный параметр относится ко всем серверам группы, независимо от того, выбрали вы серверную группу или отдельный сервер.

3 Нажмите кнопку **Настроить**.

4 Убедитесь в том, что установлен флажок «Запланировать автоматическое обновление», а затем нажмите кнопку **Расписание.**

5 Выберите параметры, задающие периодичность обновления файла описаний (например, еженедельно по вторникам в 22:00).

6 Нажмите кнопку **ОК** столько раз, сколько необходимо для возврата в главное окно Symantec System Center.

Обновление главного первичного сервера

Для ограничения каналов связи вашей сети с Интернет настройте главный первичный сервер.

Настройка главного первичного сервера

1 В окне Symantec System Center щелкните правой кнопкой мыши на сервере, и выберите команды **Все задачи** > **Symantec AntiVirus** > **Диспетчер описаний вирусов.**

2 В окне диспетчера описаний вирусов установите флажок **Обновлять первичный сервер только для этой группы.**

3 Нажмите кнопку **Настроить**.

4 В окне настройки обновлений первичного сервера нажмите кнопку **Источник**.

5 В окне настройки соединения в списке **Обновить файл описаний через** выберите **Другой защищенный сервер**, а затем при необходимости нажмите кнопку **Настроить.**

6 В окне настройки обновлений с сервера выберите в списке главный первичный сервер.

7 Нажмите кнопку **ОК.**

8 Нажмите кнопку **ОК.**

9 В окне настройки обновлений первичного сервера выполните одно из следующих действий:

- Нажмите кнопку **Обновить сейчас**, чтобы получить файл описаний вирусов с главного первичного сервера немедленно.
- Установите флажок **Запланировать автоматическое обновление**, затем нажмите кнопку **Расписание** и задайте периодичность автоматической проверки наличия обновлений на главном первичном сервере.

10 Нажмите кнопку OK столько раз, сколько необходимо для возврата в главное окно Symantec System Center.

Обновление серверов NetWare с помощью метода передачи вирусных описаний

Обновление серверов NetWare аналогично обновлению других типов серверов со следующими отличиями:

- Вы можете выделить в качестве первичного сервера сети сервер NetWare или компьютер Windows NT/2000. Если серверы NetWare работают на более быстрых компьютерах или имеют более быстрое соединение, чем серверы Windows NT/2000, то для повышения производительности вы можете выделить в качестве первичного сервера сервер NetWare.
- На главных серверах NetWare должна быть запущена поддержка TCP/IP и FTP (по умолчанию поддержка FTP на серверах NetWare выключена), и у них должно быть соединение с Интернет. Кроме того, среда NetWare требует наличия компьютера Windows NT/2000 с работающей консолью Symantec System Center.
- Серверы NetWare не хранят в своем адресном кэше адреса серверов Windows NT/2000. Если на сервере NetWare не запущена поддержка TCP/IP и этот сервер не использует DNS, то возможны затруднения при обновлении сервера NetWare с сервера Windows NT/2000, входящего в другую группу серверов.

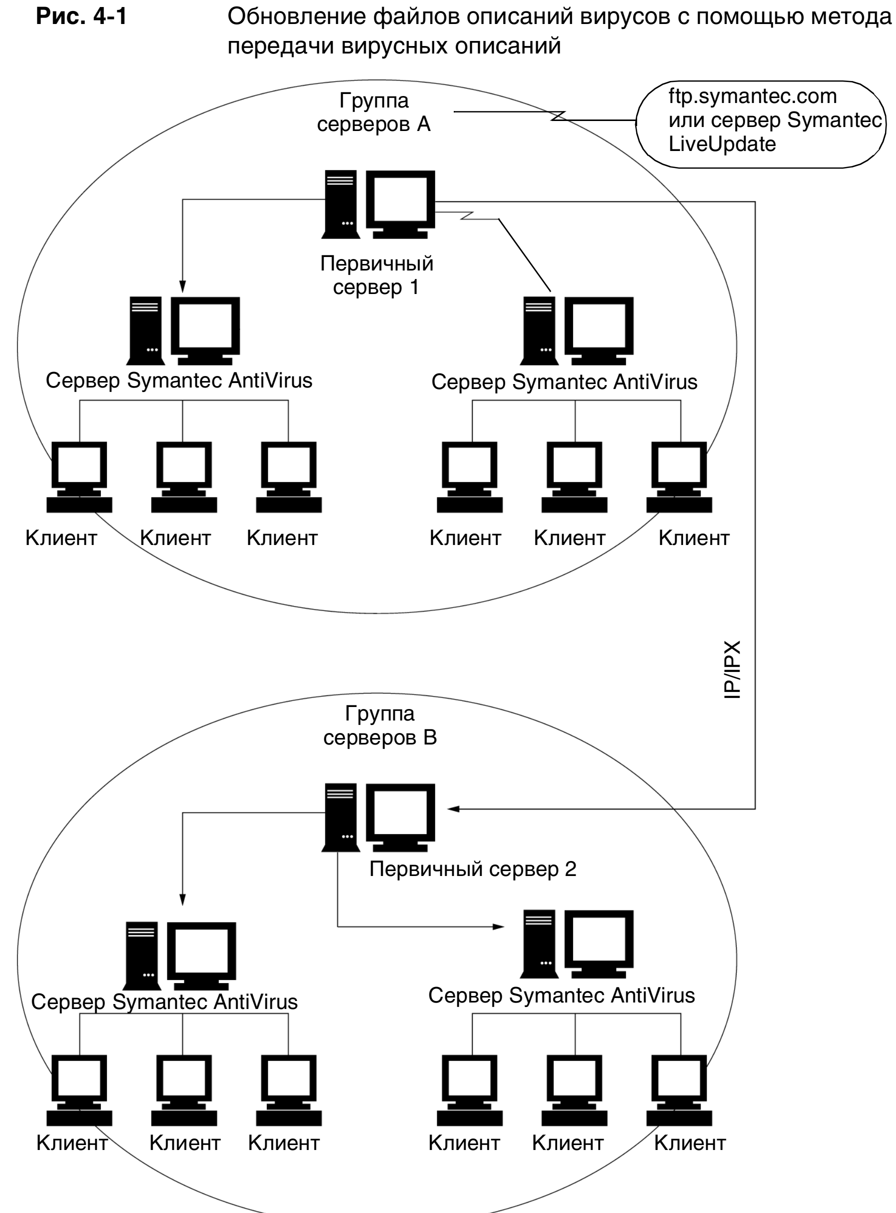
Обновление серверов NetWare без TCP/IP

◆ Временно переместите сервер NetWare в группу серверов, в которой имеется сервер Windows NT, поддерживающий протокол IPX.

Через один день этот сервер NetWare можно будет вернуть в исходную группу. В результате этих действий, адрес сервера Windows NT/2000 будет добавлен в адресный кэш сервера NetWare, что позволит этому серверу NetWare находить сервер Windows NT/2000 и получать с него обновленные описания вирусов.

На Рис. 4-1 показан пример настройки обновления файлов описаний вирусов в небольшой сети, включающей шесть файловых серверов, объединенных в две группы серверов.

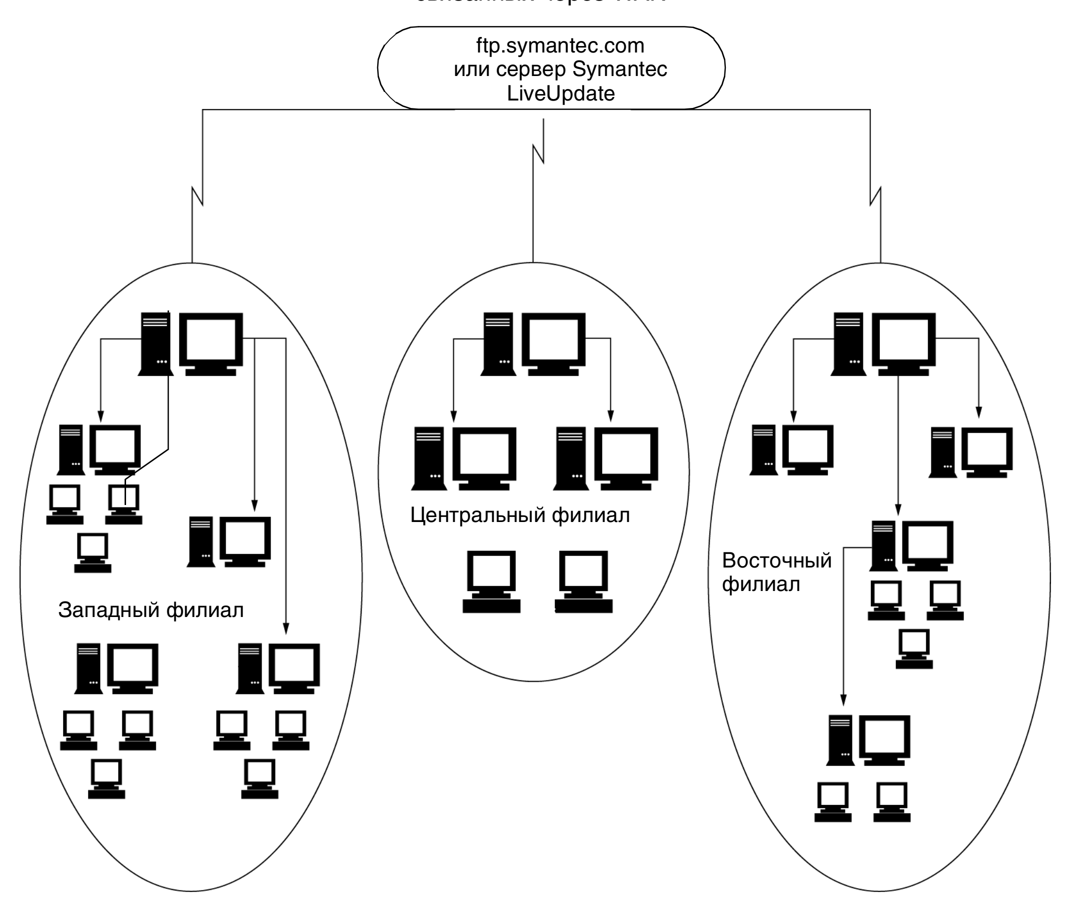
Рис. 4-1 Обновление файлов описаний вирусов с помощью метода передачи вирусных описаний



Первичный сервер получает файл описаний с FTP-сервера или с другого компьютера. Включите общий доступ к файлу описаний вирусов, чтобы серверы Symantec AntiVirus Corporate Edition из группы серверов A могли загружать последние обновления с первичного сервера 1. Клиенты будут автоматически получать обновления от родительских серверов. Первичный сервер 2 будет получать обновления с первичного сервера 1, который будет главным первичным сервером. Серверы Symantec AntiVirus Corporate Edition из группы серверов B будут получать обновления от своего первичного сервера. Клиенты будут автоматически получать обновления с серверов Symantec AntiVirus Corporate Edition.

На Рис. 4-2 показано, как можно организовать обновление файла вирусных описаний, если в вашей организации имеется несколько локальных сетей, связанных между собой через глобальную сеть (WAN).

Рис. 4-2 Обновление файлов описаний вирусов в нескольких сетях, связанных через WAN



Главные первичные серверы групп серверов в отдельных сетях получают обновления с FTP-сервера Symantec или с сервера LiveUpdate. Эти первичные серверы рассылают обновления на первичные серверы остальных групп серверов в своей локальной сети. Первичные серверы рассылают обновления другим защищенным серверам и клиентам в своей группе серверов.

Обновление серверов с помощью LiveUpdate

В зависимости от размеров вашей сети, существует два способа обновления файлов описаний вирусов с помощью LiveUpdate:

- В небольших сетях (менее 1000 узлов) рекомендуется настроить управляемые серверы для непосредственной загрузки обновлений с FTP-сайта Symantec, с сервера Symantec LiveUpdate или с внутреннего сервера LiveUpdate.
- В больших сетях (более 1000 узлов) рекомендуется настроить внутренний сервер LiveUpdate, загрузить обновления на этот сервер и разрешить управляемым серверам загрузку обновлений с внутреннего сервера LiveUpdate.

Обновление серверов Symantec AntiVirus Corporate Edition с FTP-сайта Symantec FTP или с сервера LiveUpdate

Необходимо настроить обновление для первичного сервера в каждой группе серверов, обеспечив актуальность описаний вирусов на них. Вы также можете настроить отдельные серверы для обновления непосредственно с сервера Symantec.

Обновление серверов Symantec AntiVirus Corporate Edition непосредственно с FTP-сайта Symantec или с сервера LiveUpdate

Вы можете обновить все серверы Symantec AntiVirus Corporate Edition в группе серверов с первичного сервера, либо обновлять каждый сервер в группе отдельно.

Обновление главных серверов

1. В окне Symantec System Center щелкните правой кнопкой мыши на группе серверов, и выберите команды **Все задачи** > **Symantec AntiVirus** > **Диспетчер описаний вирусов**.
2. В окне диспетчера описаний вирусов установите флажок **Обновлять первичный сервер только для этой группы**.
3. Нажмите кнопку **Настроить**.
4. В окне настройки обновлений первичного сервера выполните одно из следующих действий:
   - Нажмите кнопку **Обновить сейчас**, чтобы запустить сеанс LiveUpdate немедленно.

- Установите флажок **Запланировать автоматическое обновление**, затем нажмите кнопку **Расписание** и задайте периодичность запуска этим сервером сеансов LiveUpdate.

5 Нажмите кнопку **OK**.

6 В окне настройки обновлений первичного сервера нажмите кнопку **Источник**.

7 В списке «Обновить файл описаний через» выберите **LiveUpdate**.

8 Нажмите кнопку **OK** столько раз, сколько необходимо для возврата в главное окно Symantec System Center.

Обновление отдельных серверов с FTP-сайта Symantec FTP или с сервера LiveUpdate

1 В окне Symantec System Center щелкните правой кнопкой мыши на группе серверов, и выберите команды **Все задачи** > **Symantec AntiVirus** > **Диспетчер описаний вирусов**.

2 В окне диспетчера описаний вирусов установите флажок **Обновлять каждый сервер в этой группе серверов по отдельности**.

3 Нажмите кнопку **Настроить**.

4 В окне настройки обновлений первичного сервера нажмите кнопку **Источник**.

5 Выберите **LiveUpdate (Win32)/FTP (NetWare)**.

6 Нажмите кнопку **OK**.

Если вы настраиваете сервер NetWare, то убедитесь, что на нем запущена поддержка FTP.

7 Выполните одно из следующих действий:

- Нажмите кнопку **Обновить сейчас**, чтобы запустить сеанс LiveUpdate немедленно.
- Установите флажок **Запланировать автоматическое обновление**, затем нажмите кнопку **Расписание** и задайте периодичность запуска этим сервером сеансов LiveUpdate.

8 Нажмите кнопку **OK** столько раз, сколько необходимо для возврата в главное окно Symantec System Center.

Обновление серверов с внутреннего сервера LiveUpdate

Вы можете настроить внутренний сервер LiveUpdate на любом компьютере. Если вы применяете сервер Symantec AntiVirus Corporate Edition в качестве внутреннего сервера LiveUpdate, то для автоматического и ручного обновления файлов описаний вирусов на этом сервере вы можете применять стандартные методы обновления, перечисленные в окне диспетчера описаний вирусов. Если же в качестве внутреннего сервера LiveUpdate вы применяете компьютер, на котором не работает Symantec AntiVirus Corporate Edition, то для обновления файлов описаний вирусов на этом сервере можно применять инструмент управления LiveUpdate.

См. «Обновление серверов с помощью LiveUpdate» на стр. 138.

Дополнительные сведения приведены в книге «*LiveUpdate: Руководство администратора*».

Обновление серверов с внутреннего сервера LiveUpdate

1 В окне консоли Symantec System Center щелкните правой кнопкой мыши на группе серверов и выберите команды **Все задачи** > **LiveUpdate** > **Настройка**.

2 В окне настройки LiveUpdate выберите **Внутренний сервер LiveUpdate**.

3 Задайте следующие параметры внутреннего сервера LiveUpdate:

Имя	Имя сервера. Это имя появится при запуске сеанса LiveUpdate.
Расположение	Это поле заполнять не обязательно. В нем можно указать дополнительные сведения, относящиеся к серверу, например, адрес физического размещения сервера.
Имя (для входа в сеть)	Имя пользователя для входа на сервер. Оставьте это поле пустым, чтобы пользователи могли подключиться к серверу и получить файлы, не вводя никаких данных.
Пароль	Пароль пользователя для входа на сервер. Оставьте это поле пустым, чтобы пользователи могли подключиться к серверу и получить файлы, не вводя никаких данных.

URL или IP-адрес	■ Если вы используете метод FTP (рекомендуется), то выберите значение FTP в поле типа и введите FTP-адрес вашего сервера. Например: ftp.myliveupdateserver.com. ■ Если вы используете метод HTTP, то выберите значение HTTP в поле типа и введите URL сервера. Например: http:\\myliveupdateserver.com или 155.66.133.11\Export\Home\Ludepot ■ Если вы используете метод LAN, то выберите значение LAN в поле типа и введите путь UNC для сервера. Например: \\Myserver\LUDepot В группе «Вход в сеть» введите имя пользователя и пароль для доступа к серверу.

Если имя и пароль не указаны, то будет использоваться анонимный вход в сеть. Для этого необходимо, чтобы на FTP-сервере был разрешен анонимный вход. Если политика безопасности не допускает использование анонимного входа, то введите имя и пароль для FTP-сервера и укажите каталог, к которому будет осуществляться доступ.

4 Нажмите кнопку **OK** столько раз, сколько необходимо для возврата в главное окно Symantec System Center.

Настройка нескольких внутренних серверов LiveUpdate для повышения надежности

Для повышения надежности в случае недоступности внутреннего сервера LiveUpdate Symantec AntiVirus Corporate Edition поддерживает несколько внутренних серверов LiveUpdate.

Обновление с помощью программы Intelligent Updater

Чтобы распространить обновленные описания, загрузите новый файл Intelligent Updater, а затем используйте подходящий метод доставки обновлений управляемым серверам и клиентам. Intelligent Updater может предоставляться в виде отдельного файла или в виде нескольких небольших файлов. Доставки одним файлом предназначена для компьютеров с подключением к сети. Несколько небольших файлов можно скопировать на дискеты и использовать для обновления компьютеров, не имеющих подключения к сети или доступа к Интернет.

Обновление серверов с помощью файлов Intelligent Updater

Загрузите программу Intelligent Updater с Web-сайта Symantec и установите ее на серверы с последними файлами описаний вирусов.

Примечание: Убедитесь, что вы используете для Symantec AntiVirus Corporate Edition именно файлы Intelligent Updater, а не обычную версию продукта.

Загрузка Intelligent Updater

1. Укажите в Web-браузере следующий адрес:
   http://securityresponse.symantec.com
2. Выберите ссылку **Download Virus Definition Updates** (**Загрузить обновления описаний**).
3. Выберите ссылку **Download Updates** (**Intelligent Updater Only**) (**Загрузить описания** (**только Intelligent Updater**).
4. Выберите язык и название продукта.
5. Нажмите кнопку **Download Updates** (**Загрузить обновления**).
6. Выберите файл с расширением .Exe.
7. При появлении запроса на выбор расположения для сохранения файлов укажите папку на жестком диске.

Установка файлов описаний вирусов

1. Найдите файл Intelligent Updater, загруженный с сервера Symantec.
2. Дважды щелкните на значке этого файла и следуйте показанным на экране инструкциям.
   Если вы применяете Windows 3.1 или DOS, то после обновления нужно будет перезагрузить компьютер.
   В системах Windows 95/98/Me/NT/2000/XP делать это необязательно.

Обновление серверов с помощью опроса центрального изолятора

При использовании центрального изолятора Symantec вы можете настроить сервер центрального изолятора для периодического опроса шлюза Digital Immune System и проверки наличия обновлений. При наличии новых описаний сервер центрального изолятора может с

помощью метода передачи вирусных описаний автоматически установить эти описания на те компьютеры, которым они необходимы.

Дополнительные сведения приведены в книге «*Центральный изолятор Symantec: Руководство администратора*».

Минимизация сетевого трафика и обработка пропущенных обновлений

LiveUpdate содержит ряд дополнительных параметров, позволяющих минимизировать сетевой трафик и обрабатывать пропущенные обновления. В Табл. 4-2 описаны параметры планирования LiveUpdate.

Табл. 4-2 Параметры планирования LiveUpdate

Параметр	Описание	Рекомендации по применению
Параметры рандомизации	Рандомизация обновлений: ■ Обновление выполняется в пределах заданного интервала от запланированного времени (плюс или минус указанное число минут) ■ Обновление выполняется в любой день недели в пределах указанного интервала времени. ■ Обновление выполняется в любой день месяца в пределах определенного количества дней до или после заданной даты.	Вы можете разнести во времени обновление нескольких компьютеров для более равномерного распределения сетевого трафика. По умолчанию Symantec AntiVirus Corporate Edition выполняет рандомизацию сеансов LiveUpdate для снижения пиковых нагрузок на сеть.

Табл. 4-2 Параметры планирования LiveUpdate

Параметр	Описание	Рекомендации по применению
Параметры обработки пропущенных событий	Эти параметры определяют обработку пропущенных событий LiveUpdate. Событие может быть пропущено из-за того, что компьютер выключен в тот момент времени, на который запланирован запуск сеанса LiveUpdate. Имеется возможность настроить параметры так, чтобы пропущенные операции LiveUpdate выполнялись позднее.	Таким образом можно гарантировать, что компьютеры, недоступные в момент регулярного планового обновления LiveUpdate, в дальнейшем попытаются получить обновленные описания.

Минимизация сетевого трафика и обработка пропущенных обновлений

Для снижения нагрузки на сеть вы можете настроить разные параметры рандомизации для планового обновления клиентов и серверов Symantec AntiVirus Corporate Edition.

Вы также можете задать разные политики обработки пропущенных событий LiveUpdate для клиентов и серверов Symantec AntiVirus Corporate Edition.

Настройка рандомизации расписания LiveUpdate для серверов

1. В окне Symantec System Center щелкните правой кнопкой мыши на сервере или группе серверов, и выберите команды **Все задачи** > **Symantec AntiVirus** > **Диспетчер описаний вирусов**.
2. В окне диспетчера описаний вирусов нажмите кнопку **Настройка**.
3. В окне настройки обновлений для первичного сервера установите флажок **Запланировать автоматическое обновление**.
4. Нажмите кнопку **Расписание**.
5. Задайте периодичность и время проверки наличия обновлений этим сервером.
6. В окне диспетчера описаний вирусов нажмите кнопку **Дополнительно**.

7 В окне дополнительных параметров расписания в группе параметров рандомизации выберите **Параметры** и укажите параметры минут, дня недели и дня месяца.

8 Нажмите кнопку **OK** столько раз, сколько необходимо для возврата в главное окно Symantec System Center.

Настройка рандомизации расписания LiveUpdate для клиентов

1 В окне консоли Symantec System Center щелкните правой кнопкой мыши на сервере или группе серверов, и выберите команды **Все задачи** > **Symantec AntiVirus** > **Диспетчер описаний вирусов**.

2 В окне диспетчера описаний вирусов выберите параметр **Автоматическое обновление клиентами описаний вирусов с помощью LiveUpate**.

3 В окне расписания диспетчера описаний вирусов нажмите кнопку **Расписание**.

4 Задайте периодичность и время проверки наличия обновлений клиентами.

5 Нажмите кнопку **Дополнительно**.

6 В окне дополнительных параметров расписания в группе параметров рандомизации выберите **Параметры** и укажите параметры минут, дня недели и дня месяца.

7 Нажмите кнопку **OK** столько раз, сколько необходимо для возврата в главное окно Symantec System Center.

Настройка обработки пропущенных событий LiveUpdate для серверов

1 В окне консоли Symantec System Center щелкните правой кнопкой мыши на сервере или группе серверов, и выберите команды **Все задачи** > **Symantec AntiVirus** > **Диспетчер описаний вирусов**.

2 В окне диспетчера описаний вирусов нажмите кнопку **Настройка**.

3 Установите флажок **Запланировать автоматическое обновление**.

4 В окне настройки обновлений первичного сервера нажмите кнопку **Расписание**.

5 В окне диспетчера описаний вирусов нажмите кнопку **Дополнительно**.

6 В окне дополнительных параметров расписания выберите **Обрабатывать пропущенные события не позднее**.

7 Задайте промежуток времени, в течение которого будет возможен запуск пропущенной операции.

Например, можно разрешить запуск еженедельного сеанса LiveUpdate в течение трех дней после момента времени, заданного для выполнения этой операции.

8 Нажмите кнопку **ОК** столько раз, сколько необходимо для возврата в главное окно Symantec System Center.

Настройка обработки пропущенных событий LiveUpdate для клиентов

1 В окне консоли Symantec System Center щелкните правой кнопкой мыши на сервере или группе серверов, и выберите команды **Все задачи** > **Symantec AntiVirus** > **Диспетчер описаний вирусов**.

2 В окне диспетчера описаний вирусов выберите параметр **Автоматическое обновление клиентами описаний вирусов с помощью LiveUpate**.

3 Нажмите кнопку **Расписание**.

4 В окне диспетчера описаний вирусов нажмите кнопку **Дополнительно**.

5 Установите флажок **Обрабатывать пропущенные события не позднее**.

6 Задайте промежуток времени, в течение которого будет возможен запуск пропущенной операции.

7 Нажмите кнопку **ОК** столько раз, сколько необходимо для возврата в главное окно Symantec System Center.

Например, можно разрешить запуск еженедельного сеанса LiveUpdate в течение трех дней после момента времени, заданного для выполнения этой операции.

Обновление файлов описаний вирусов на клиентах Symantec AntiVirus Corporate Edition

Для обновления файлов описаний вирусов на клиентах Symantec AntiVirus Corporate Edition можно применять следующие методы:

- Метод передачи вирусных описаний
- Функция LiveUpdate

- Intelligent Updater

  См. «Настройка нескольких внутренних серверов LiveUpdate для повышения надежности» на стр. 141.

- Опрос центрального изолятора

  См. «Обновление серверов с помощью опроса центрального изолятора» на стр. 142.

См. «Методы обновления файлов описаний вирусов» на стр. 130.

Обновление файлов описаний вирусов на клиентах Symantec AntiVirus Corporate Edition

Вы можете обновлять файлы описаний вирусов на клиентах Symantec AntiVirus Corporate Edition с помощью метода передачи вирусных описаний, с помощью LiveUpdate или с помощью обоих методов.

Обновление клиентов с помощью метода передачи вирусных описаний

1. В окне консоли Symantec System Center щелкните правой кнопкой мыши на группе серверов и выберите команды **Все задачи** > **Symantec AntiVirus** > **Диспетчер описаний вирусов**.
2. В окне диспетчера описаний вирусов выберите команду **Обновлять описания с родительского сервера**.
3. Нажмите кнопку **Настройка**.
4. В окне параметров обновления задайте частоту установки обновлений родительским сервером.
5. Нажмите кнопку **OK**.
6. В окне диспетчера описаний вирусов отмените выбор параметра **Автоматическое обновление клиентами описаний вирусов с помощью LiveUpate**.
7. Нажмите кнопку **OK** столько раз, сколько необходимо для возврата в главное окно Symantec System Center.

Обновление клиентов с помощью LiveUpdate

1. В окне консоли Symantec System Center щелкните правой кнопкой мыши на группе серверов и выберите команды **Все задачи** > **Symantec AntiVirus** > **Диспетчер описаний вирусов**.

2 В окне диспетчера описаний вирусов выберите параметр **Автоматическое обновление клиентами описаний вирусов с помощью LiveUpate**.

3 Нажмите кнопку **Расписание**.

4 В окне расписания обновления описаний вирусов задайте частоту, день и время обновления.

5 Нажмите кнопку **ОК** столько раз, сколько необходимо для возврата в главное окно Symantec System Center.

Обновление клиентов с помощью метода передачи вирусных описаний и LiveUpdate

1 В окне консоли Symantec System Center щелкните правой кнопкой мыши на группе серверов и выберите команды **Все задачи** > **Symantec AntiVirus** > **Диспетчер описаний вирусов**.

2 В окне диспетчера описаний вирусов выберите **Обновлять описания с родительского сервера**.

3 Установите флажок **Регулярное автоматическое обновление LiveUpdate**.

4 Нажмите кнопку **Расписание**.

5 В окне расписания обновления описаний вирусов задайте частоту, день и время обновления.

6 Нажмите кнопку **ОК**.

7 Нажмите кнопку **Настройка**.

8 В окне параметров обновления задайте частоту установки обновлений родительским сервером.

9 Нажмите кнопку **ОК** столько раз, сколько необходимо для возврата в главное окно Symantec System Center.

Настройка управляемых клиентов для применения внутреннего сервера LiveUpdate

Вы можете с помощью Symantec System Center настроить параметры LiveUpdate для управляемых компьютеров, применяющих клиента Symantec AntiVirus Corporate Edition. Для автономных клиентов Symantec AntiVirus Corporate Edition следует создать пользовательский файл .Hst с помощью программы управления LiveUpdate.

Информация о настройке LiveUpdate для автономных клиентов Symantec AntiVirus Corporate Edition приведена в справке по программе управления LiveUpdate.

Настройка управляемых клиентов Symantec AntiVirus Corporate Edition для применения внутреннего сервера LiveUpdate

1 Щелкните правой кнопкой мыши на родительском сервере и выберите команды **Все задачи** > **LiveUpdate** > **Настройка**.

2 В окне настройки LiveUpdate выберите **Внутренний сервер LiveUpdate**.

3 Если вы применяете сервер FTP или HTTP, то укажите необходимые значения в полях имени и пароля.

4 В поле подключения введите одно из следующих значений:
   - Путь UNC к общей папке
   - URL или IP-адрес сервера FTP или HTTP

5 В списке «Тип» выберите одно из следующих значений:
   - LAN
   - FTP
   - HTTP

6 Нажмите кнопку **ОК** столько раз, сколько необходимо для возврата в главное окно Symantec System Center.

   Если вы применяете несколько родительских серверов, то повторите шаги 1–6 для каждого родительского сервера, чтобы изменения были применены на всех клиентах и серверах Symantec AntiVirus Corporate Edition. Вы также можете настроить LiveUpdate для всей группы серверов, щелкнув на ней правой кнопкой мыши.

Включение и настройка постоянного обновления управляемых клиентов с помощью LiveUpdate

Если управляемый клиент Symantec AntiVirus Corporate Edition редко подключается к своему родительскому серверу (такое возможно, например, при работе с портативным компьютером), то он может не получить последние обновления файлов описаний вирусов. Для таких компьютеров предусмотрена функция постоянного обновления с помощью LiveUpdate, позволяющая получать обновления непосредственно с сервера Symantec при подключении компьютера к Интернет.

При использовании функции постоянного обновления с помощью LiveUpdate вы можете задать максимальное число дней, на протяжении которых компьютер Symantec AntiVirus Corporate Edition может применять устаревшие файлы описаний вирусов, после чего выполняется обязательное обновление. Когда клиент Symantec AntiVirus Corporate Edition определяет, что возраст его файлов описаний достиг заданного ограничения, то при очередном подключении к Интернет он начинает сеанс LiveUpdate, не требующий вмешательства пользователя.

Включение и настройка постоянного обновления с помощью LiveUpdate

Для включения постоянного обновления с помощью LiveUpdate вы можете воспользоваться Symantec System Center или редактором реестра на клиентах Symantec AntiVirus Corporate Edition. После этого вы можете настроить параметры постоянного обновления с помощью LiveUpdate, добавив значения в реестр клиента.

Включение постоянного обновления с помощью LiveUpdate из Symantec System Center

1. В окне консоли Symantec System Center щелкните правой кнопкой мыши на клиенте, сервере, группе клиентов или группе серверов Symantec AntiVirus Corporate Edition, и выберите команды **Все задачи** > **Symantec AntiVirus** > **Диспетчер описаний вирусов**.
2. В окне диспетчера описаний вирусов установите флажок **Включить постоянное обновление с помощью LiveUpdate**.
3. Нажмите кнопку **OK** столько раз, сколько необходимо для возврата в главное окно Symantec System Center.

Включение постоянного обновления с помощью LiveUpdate путем редактирования реестра

1. С помощью редактора реестра Regedit найдите следующий ключ: HKEY_LOCAL_MACHINE\SOFTWARE\INTEL\LANDesk\VirusProtect6\CurrentVersion\PatternManager
2. Добавьте новый параметр EnableAdminForcedLU типа DWORD.
3. Присвойте этому параметру одно из следующих значений:
   - 1: Включено
   - 0: Выключено

Настройка постоянного обновления с помощью LiveUpdate

◆ Для настройки постоянного обновления с помощью LiveUpdate применяются следующие ключи реестра:

EnableAdminForcedLU	Укажите 0, если необходимо выключить постоянное обновление с помощью LiveUpdate, или 1, если необходимо включить его.
MaxDefsDaysOldAllowed	Укажите максимальный возраст файлов описаний (в днях), после которого Symantec AntiVirus Corporate Edition должен запускать сеанс LiveUpdate.
AdminForcedLUCheckInterval	Укажите интервал проверки старых определений (в секундах).
AFLUDelay	Задайте задержку запуска функции постоянного обновления с помощью LiveUpdate (от 10 до 180 минут). Это время задержки действует лишь в том случае, если данная функция включена. Фактическое время задержки будет представлять собой случайное число в диапазоне от 8 до N+8, где N — это значение, указанное в реестре. По умолчанию задано значение 30 минут.

Примечание: В параметре MaxDefsDaysOldAllowed должно быть указано значение не менее 8 дней. Меньшее значение может привести к возникновению неполадок при попытке вернуться к предыдущей версии файлов описаний вирусов, поскольку возраст файлов, к которым вы планируете вернуться, может оказаться больше числа дней, разрешенного функцией постоянного обновления LiveUpdate.

Настройка правил использования функции LiveUpdate

Можно настроить правила использования LiveUpdate управляемыми клиентами. Если эти правила включены, то соответствующие функции недоступны для клиентов. Этими правилами определяется, могут ли выполняться перечисленные ниже действия на уровне клиента.

- Изменение расписания LiveUpdate
- Запуск LiveUpdate вручную

Настройка правил использования LiveUpdate

1. В окне консоли Symantec System Center щелкните правой кнопкой мыши на сервере или группе серверов, и выберите команды **Все задачи** > **Symantec AntiVirus** > **Диспетчер описаний вирусов**.
2. Выполните одно из следующих действий:
   - Чтобы клиенты не могли изменять расписание сеансов LiveUpdate, установите флажок **Запретить клиентам изменять расписание LiveUpdate**. (Чтобы этот флажок стал доступен, необходимо установить флажок «Регулярное автоматическое обновление LiveUpdate»).
   - Для запрета обновления приложения снимите флажок **Загрузить обновления продукта с помощью LiveUpdate**.
   - Для того чтобы клиенты не могли запускать сеансы LiveUpdate вручную, установите флажок **Запретить клиентам ручной запуск LiveUpdate**.

Примечание: Если флажок «Запретить клиентам изменять расписание LiveUpdate» или флажок «Запретить клиентам ручной запуск LiveUpdate» не установлен, то клиент сможет запустить сеанс LiveUpdate в любое время.

Управление файлами описаний вирусов

Консоль Symantec System Center содержит ряд инструментов, предназначенных для управления установкой файлов описаний вирусов в сети. Эти инструменты позволяют выполнять следующие операции:

- Проверка даты выпуска файла описаний вирусов на серверах
- Просмотр списков вирусов на серверах и клиентах
- Возврат к предыдущей версии файлов описаний вирусов в пределах всей сети

Если применение новых файлов описаний вирусов приводит к возникновению ложных срабатываний системы защиты или к другим неполадкам на сервере, то вы можете проверить номер версии файлов описаний вирусов на этом сервере, а затем с помощью Symantec System Center вернуть более ранний набор описаний. Все серверы и клиенты группы серверов вернутся к использованию указанной вами версии файлов описаний вирусов. Имеется возможность выбирать версию файлов описаний вирусов для всех серверов и клиентов, входящих в группу

серверов. Пользователей, загрузивших файлы описаний, которые еще не допущены к использованию на вашем предприятии, можно принудительно вернуть к использованию указанной вами версии. Поскольку отмена установки новых файлов описаний вирусов является очень простой процедурой, вы можете выпускать новые файлы описаний вирусов за меньшее время.

Symantec System Center показывает значок предупреждения для тех компьютеров, управляемых родительским сервером, группой серверов или группой клиентов, на которых применяются устаревшие файлы описаний вирусов.

Поиск компьютера с устаревшими описаниями

- Разверните сервер, группу серверов или группу клиентов и найдите значки предупреждений.

Проверка номера версии файлов описаний вирусов

С помощью Symantec System Center вы можете определить номер версии файлов описаний вирусов на сервере, клиенте, группе серверов или группе клиентов Symantec AntiVirus Corporate Edition.

Проверка номера версии файлов описаний вирусов

- В окне Symantec System Center щелкните правой кнопкой мыши на группе серверов, группе клиентов, сервере или клиенте Symantec AntiVirus Corporate Edition, и выберите команду **Свойства**.

  На вкладке Symantec AntiVirus в группе **Описания вирусов** указана дата и версия файла описания вирусов.

  После обновления файлов описаний может пройти несколько минут, прежде чем новые данные будут отражены в окне консоли.

Просмотр списка вирусов

Имеется возможность просмотреть список известных вирусов на выбранном сервере или клиенте. Список вирусов позволяет убедиться, что данный компьютер защищен от того или иного конкретного вируса.

Просмотр списка вирусов

- Щелкните правой кнопкой мыши на сервере или клиенте, а затем выберите команды **Все задачи** > **Symantec AntiVirus** > **Просмотр списка вирусов**.

Возврат к предыдущей версии файлов описаний вирусов

При необходимости, можно вернуться к использованию предыдущей версии файлов описаний вирусов для группы серверов. Это может потребоваться, например, в том случае, если новые файлы приводят к ложному обнаружению вирусов.

Примечание: Когда вы возвращаетесь к использованию предыдущих версий файлов описаний вирусов, то описания, выпущенные позже, чем включенные в предыдущую версию, удаляются.

Возврат к предыдущей версии файлов описаний вирусов

1 В окне консоли Symantec System Center щелкните правой кнопкой мыши на сервере или группе серверов, и выберите команды **Все задачи** > **Symantec AntiVirus** > **Диспетчер описаний вирусов**.

2 В окне диспетчера описаний вирусов установите флажок «Обновлять первичный сервер только для этой группы» и нажмите кнопку **Настроить**.

3 В окне настройки обновлений первичного сервера нажмите кнопку **Файл описаний**.

4 В окне выбора файла описаний вирусов укажите файл, к которому необходимо вернуться, и нажмите кнопку **Применить**.

5 Нажмите кнопку **Да**, чтобы подтвердить переход к другому файлу.

6 Нажмите кнопку **ОК** столько раз, сколько необходимо для возврата в главное окно Symantec System Center.

Тестирование файлов описаний вирусов

Многие администраторы проводят предварительное тестирование файлов описаний в специально выделенной сети перед их установкой на основной сервер предприятия. Для тестирования файлов описаний вирусов выполните следующие действия:

- Установите сервер Symantec AntiVirus Corporate Edition на первичный сервер тестовой сети.
- С первичного сервера тестовой сети запустите функцию LiveUpdate, чтобы загрузить новый файл описаний.

- Загрузите с сайта www.eicar.org тестовый файл, позволяющий проверить работу файла описаний вирусов.
- После завершения тестирования скопируйте файл описаний вирусов из папки \Program files\Nav тестового сервера в аналогичную папку на первичных серверах рабочей сети.
- Когда файл описаний будет загружен на первичные серверы, другие серверы, входящие в группы серверов, тоже смогут получить этот файл.

Примечание: Клиенты будут автоматически получать описания со своих родительских серверов, если установлен флажок «Обновлять описания с родительского сервера» в окне «Диспетчер описаний вирусов».

Примеры обновления

В следующих примерах проиллюстрированы процедуры обновления, применяемые администраторами двух различных компаний.

- В компании А администратор загружает новые описания с FTP-сервера компании Symantec или с сервера Symantec LiveUpdate на первичный сервер тестовой сети. Он проводит тестирование загруженного файла описаний. Завершив тестирование, он копирует файл описаний на главный первичный сервер основной сети компании. Другие первичные серверы он настроил на получение обновлений с главного первичного сервера. Все остальные подключенные компьютеры используют метод передачи вирусных описаний. Вторичные серверы получают обновления со своих первичных серверов. Клиенты получают обновления со своих родительских серверов. (Клиенты Windows 3.1 и DOS получают обновления при следующем входе в систему).
- В компании Б администратор загружает новые описания с FTP-сервера компании Symantec или с сервера Symantec LiveUpdate в тестовую сеть. Он проводит тестирование загруженного файла описаний. Завершив тестирование, администратор загружает новые описания с FTP-сервера компании Symantec или с сервера Symantec LiveUpdate на внутренний сервер LiveUpdate основной сети. Некоторым пользователям, риск заражения которых невысок, разрешается выход за брандмауэр. Когда они запускают сеансы LiveUpdate на своих компьютерах, файлы описаний вирусов загружаются прямо с FTP-сайта компании Symantec или с сервера Symantec LiveUpdate.

Глава 5

Реакция на массовое заражение

Эта глава содержит следующие разделы:

Сведения о реакции на массовое заражение

Реакция на массовое заражение требует заблаговременной подготовки и наличия стратегии, позволяющей адекватно отреагировать на это событие.

Помимо установки Symantec AntiVirus Corporate Edition на серверы и рабочие станции сети, подготовка к реакции на заражение включает также следующие задачи:

- Создание и анализ плана реакции на заражение
- Определение действий Symantec AntiVirus Corporate Edition по обработке вирусов
- Стратегия реакции на заражение включает следующие компоненты:
  - Включение предупреждений и сообщений о вирусах
  - Выполнение сплошной проверки сети
  - Отслеживание вирусов с помощью журналов
  - Применение консоли центрального изолятора для отслеживания зараженных компьютеров в вашей сети и передачи подозрительных файлов в центр Symantec Security Response для анализа и исправления.

Подготовка к реакции на заражение

Для правильной реакции на заражение необходимо создать план и разработать действия по обработке подозрительных файлов.

Создание плана реакции на заражение

Эффективный ответ на заражение сети вирусами требует наличия плана, позволяющего действовать быстро и эффективно.

Табл. 5-1 содержит список задач по созданию плана реакции на заражение.

Табл. 5-1 Модель плана реакции на заражение

Задача	Описание
Обеспечение загрузки обновленных файлов описаний вирусов.	На зараженных компьютерах должны быть установлены последние версии файлов описаний вирусов. При необходимости установите новые описания на компьютеры с помощью метода передачи вирусных описаний. См. «Сведения о файлах описаний вирусов» на стр. 130.
Создание схемы топологии сети.	Подготовьте схему топологии сети, позволяющую систематически изолировать отдельные сегменты сети и удалять вирусы с находящихся в них компьютеров перед повторным подключением этих компьютеров к локальной сети. Схема должна включать следующие сведения: ■ Имена и адреса серверов ■ Имена и адреса клиентов ■ Список сетевых протоколов ■ Список общих ресурсов
Идентификация вируса.	Наилучшим источником информации о вирусах, обнаруженных в вашей сети, являются журналы Symantec AntiVirus Corporate Edition. Вы можете идентифицировать вирус с помощью журналов вирусов или обратиться к энциклопедии вирусов Symantec Security Response и определить, как лучше всего удалить вирус.
Реакция на появление неизвестных вирусов.	Если после анализа журналов вы не можете идентифицировать подозрительный файл как зараженный вирусом, и после установки последних описаний вирусов файл не был исправлен, то посетите Web-сайт http://securityresponse.symantec.com и просмотрите новости, опубликованные в разделах «Latest Virus Threats» и «Security Advisories».

Табл. 5-1 Модель плана реакции на заражение

Задача	Описание
Знакомство с технологиями обеспечения безопасности.	Помимо знакомства с топологией сети вы также должны быть знакомы с реализацией в вашей организации Symantec AntiVirus Corporate Edition и других продуктов обеспечения безопасности, применяемых в сети. Вы должны знать ответы на следующие вопросы: ■ Какие программы обеспечения безопасности защищают сетевые серверы и рабочие станции? ■ Каково применяемое расписание обновления описаний вирусов? ■ Какие альтернативные методы получения обновлений будут доступны в случае атаки обычных каналов рассылки? ■ Какие файлы журналов доступны для отслеживания вирусов в вашей сети?
Наличие плана восстановления из резервной копии.	В случае массового катастрофического заражения вирусами может потребоваться восстановление серверов и клиентов, чтобы гарантировать работу сети. Наличие плана восстановления критически важных компьютеров из резервной копии может оказаться крайне важным.

Определение действий Symantec AntiVirus Corporate Edition для обработки подозрительных файлов

По умолчанию при обнаружении подозрительного файла Symantec AntiVirus Corporate Edition выполняет следующие действия:

- Symantec AntiVirus Corporate Edition пытается исправить файл.
- Если файл невозможно исправить с помощью текущего набора описаний вирусов, то зараженный файл перемещается в изолятор на локальном компьютере. Кроме того, клиент Symantec AntiVirus Corporate Edition создает в журнале запись об обнаружении вируса. Данные клиента Symantec AntiVirus Corporate Edition передаются первичному серверу. Вы можете просмотреть данные журнала с консоли Symantec System Center.

Для завершения стратегии обработки вирусов вы также можете выполнить следующие дополнительные действия:

- Определить различные действия по восстановлению для разных типов вирусов. Например, можно настроить Symantec AntiVirus Corporate Edition таким образом, чтобы он автоматически удалял макровирусы, но при обнаружении программного вируса выдавал запрос о применяемом действии.
- Выбрать резервное действие для файлов, которые Symantec AntiVirus Corporate Edition не может исправить, например, удаление зараженного файла.
- Получать предупреждения о вирусах, например, с помощью пейджера или электронной почты при использовании системы AMS[2].
- Настроить локальный изолятор для пересылки зараженных файлов в центральный изолятор. Вы можете настроить центральный изолятор таким образом, чтобы он пытался исправить зараженные файлы с помощью своих файлов описаний вирусов (которые могут быть более новыми, чем описания на локальном компьютере), либо чтобы он автоматически пересылал зараженные файлы в центр Symantec Security Response для анализа.

См. «Сведения о системе Alert Management System» на стр. 52.

Дополнительные сведения приведены в книге «*Центральный изолятор Symantec: Руководство администратора*».

Автоматическое удаление подозрительных файлов из локального изолятора

Когда Symantec AntiVirus Corporate Edition проверяет подозрительный файл, этот файл помещается в папку локального изолятора на зараженном компьютере. Функция очистки изолятора автоматически удаляет из изолятора файлы, находящиеся там дольше установленного времени.

Очисткой изолятора управляет следующий ключ реестра:

\\HKEY_LOCAL_MACHINE\SOFTWARE\INTEL\LANDesk\VirusProtect6\CurrentVersion\Quarantine

Табл. 5-2 содержит список возможных параметров очистки изолятора.

Табл. 5-2 Параметры очистки изолятора

Параметр	Значение	Описание
QuarantinePurgeEnabled	0/1	Выключить/включить очистку
QuarantinePurgeAgeLimit	X	Задает максимальное время хранения файлов в каталоге изолятора (в днях)
QuarantinePurgeFrequency	X	Задает частоту удаления: 0=дни, 1=месяцы, 2=годы
BackupItemPurgeEnabled	0/1	Выключает/включает удаление файлов резервных копий
BackupItemPurgeAgeLimit	X	Задает максимальное время хранения файлов резервных копий в изоляторе (в днях)
BackupItemPurgeFrequency	X	Задает частоту удаления файлов резервных копий: 0=дни, 1=месяцы, 2=годы
RepairedItemPurgeEnabled	0/1	Выключает/включает удаление исправленных файлов
RepairedItemPurgeFrequency	X	Задает частоту удаления исправленных файлов: 0=дни, 1=месяцы, 2=годы

Реакция на заражение сети

Symantec AntiVirus Corporate Edition предоставляет следующие инструменты, позволяющие реагировать на заражение сети:

- Предупреждения: Отправляет встроенные предупреждения и предупреждения AMS[2]
- Сплошная проверка: Выполняет проверку структуры системы, группы серверов или отдельного сервера
- Журналы событий: Позволяет отслеживать вирусы и операции отправки файлов в центральный изолятор на уровне группы сервера, отдельного сервера или клиента

- Консоль центрального изолятора: Позволяет отслеживать операции отправки файлов в центр Symantec Security Response
- Диск аварийного восстановления: Позволяет очистить загрузочный сектор от вирусов

Применение предупреждений и сообщений о вирусах

Предупреждения и сообщения позволяют получать информацию о подозрительных файлах, обнаруженных Symantec AntiVirus Corporate Edition в сети. Symantec AntiVirus Corporate Edition содержит следующие механизмы уведомления:

- AMS^2: Если эта система настроена, то клиенты Symantec AntiVirus Corporate Edition смогут передавать серверам AMS^2 события, связанные с обнаружением вирусов. Вы можете настроить серверы AMS^2 для отправки предупреждений на пейджер, для отправки сообщений электронной почты или для использования других механизмов уведомления.

  См. «Сведения о системе Alert Management System» на стр. 52.

- Пользовательские сообщения: С помощью консоли Symantec System Center вы можете настроить пользовательское сообщение, которое должно появляться на клиентах Symantec AntiVirus Corporate Edition при обнаружении подозрительного файла.

  См. «Настройка и вывод сообщения на экран зараженного компьютера» на стр. 110.

Выполнение сплошной проверки

В случае обнаружения подозрительных файлов трудно определить, связана ли возникшая проблема только с тем компьютером или сервером, на котором эти файлы обнаружены, или заражение могло распространиться на другие области сети. В этом случае целесообразно выполнить сплошную проверку с помощью Symantec System Center. Количество осматриваемых компьютеров зависит от способа запуска проверки.

Если клиент Symantec AntiVirus Corporate Edition недоступен во время сплошной проверки, то Symantec AntiVirus Corporate Edition выполнит одно из следующих действий:

- В 32-разрядных операционных системах: Компьютер будет проверен сразу после включения. Вход в сеть необязателен.
- В 16-разрядных операционных системах: Компьютер будет проверен сразу после включения и входа в сеть.

В зависимости от объекта, выбранного в окне консоли Symantec System Center, вы можете запустить сплошную проверку всей сети, группы серверов или отдельного сервера.

Предупреждение: Сплошная проверка может существенно увеличить сетевой трафик, причем объем данных и продолжительность операции будут зависеть от размеров вашей сети. Запущенная сплошная проверка должна завершиться, остановить ее нельзя.

Запуск сплошной проверки

1. В окне Symantec System Center щелкните правой кнопкой мыши на сети, группе серверов или на отдельном сервере, и выберите команды **Все задачи** > **Symantec AntiVirus** > **Начать сплошную проверку**.
2. Введите название проверки.
3. Нажмите кнопку **Пуск**.

   См. «Настройка параметров осмотра» на стр. 106.

Отслеживание предупреждений о вирусах с помощью журналов

Вы можете просматривать предупреждения об обнаружении вирусов с помощью консоли Symantec System Center. По умолчанию предупреждения об обнаружении вирусов сохраняются в течение трех дней. Вы можете изменить число дней хранения предупреждений.

См. «Сведения о журналах» на стр. 184.

Отслеживание операций передачи файлов в Symantec Security Response с консоли центрального изолятора

Консоль Symantec System Center заносит в журнал событий информацию о всех операциях передачи клиентом Symantec AntiVirus Corporate Edition подозрительных файлов в центр Symantec Security Response. Помимо записей журналов, вы можете отслеживать состояние операций передачи файлов в центр Symantec Security Response в реальном времени с помощью консоли центрального изолятора.

Информация о работе с консолью центрального изолятора приведена в книге «*Центральный изолятор Symantec: Руководство администратора*».

Глава 6

Управление перемещающимися клиентами

Эта глава содержит следующие разделы:

Сведения о перемещающихся клиентах

Перемещающийся клиент может выполнять следующие операции:

- Автоматически находить наилучший родительский сервер в зависимости от скорости сети и расстояния, и настраиваться в качестве управляемого клиента этого родительского сервера. Например, когда мобильный пользователь переезжает из Москвы в Новосибирск, то функция перемещающегося клиента определяет новый сетевой адрес выбирает для портативного компьютера наилучший родительский сервер.
- При изменении сетевого адреса подключаться к ближайшему родительскому серверу.
- Переключаться на другой родительский сервер, если текущий родительский сервер стал недоступным.
- Периодически проверять, какой родительский сервер является ближайшим, что позволяет изменять настройку в соответствии с изменением в конфигурации серверов и в уровне нагрузки.
- При выборе родительского сервера в наборе эквивалентных серверов пытаться выровнять уровень загрузки различных серверов.
- При преобразовании автономных клиентов в управляемых клиентов автоматически определять наилучший родительский сервер при подключении клиента к сети. Например, корпорация может иметь центр распространения для новых компьютеров. Перед отправкой компьютеров в региональные филиалы администраторы включают на компьютерах поддержку роуминга. Эта операция включает в себя указание всех возможных серверов для новых компьютеров. Когда пользователи подключают новые компьютеры к сети, Symantec AntiVirus Corporate Edition автоматически выберет для них наилучшие родительские серверы.

Компоненты перемещающихся клиентов

В Табл. 6-1 перечислены компоненты перемещающихся клиентов.

Табл. 6-1 Компоненты перемещающихся клиентов

Компонент	Описание
Список серверов нулевого уровня	Список серверов нулевого уровня, доступных для применения в качестве серверов роуминга для выбранного перемещающегося клиента. Перемещающиеся клиенты хранят эти данные в своем реестре. См. «Анализ сети Symantec AntiVirus Corporate Edition и составление ее схемы» на стр. 169. См. «Создание списка серверов Symantec AntiVirus Corporate Edition нулевого уровня» на стр. 170.
Иерархический список серверов	Список всех серверов роуминга, сгруппированных в виде иерархической структуры. Серверы роуминга хранят эти данные в своем реестре. См. «Анализ сети Symantec AntiVirus Corporate Edition и составление ее схемы» на стр. 169. См. «Создание иерархического списка серверов Symantec AntiVirus Corporate Edition» на стр. 171.
Roamadmn.exe	Настраивает серверы роуминга Symantec AntiVirus Corporate Edition для доступа перемещающихся клиентов. См. «Настройка поддержки роуминга на серверах роуминга» на стр. 174.
Navroam.exe	Предоставляет перемещающимся клиентам данные о серверах роуминга. См. «Настройка поддержки роуминга на перемещающихся клиентах» на стр. 171.

Как работает роуминг

Функция поддержки перемещающихся клиентов применяет два типа списков: Один или несколько списков серверов нулевого уровня и иерархический список серверов, которые должны поддерживать перемещающихся клиентов. Перемещающиеся клиенты хранят список серверов нулевого уровня в своем реестре и используют его для идентификации серверов, к которым следует пытаться подключиться.

Реализацию роуминга в сети следует начинать с подготовки одного или нескольких списков серверов нулевого уровня и иерархического списка серверов. После рассылки этих данных перемещающиеся клиенты будут работать в соответствии со следующим алгоритмом:

- При загрузке клиента Symantec AntiVirus Corporate Edition на нем запускается программа Navroam.exe, выбирающая наилучший сервер Symantec AntiVirus Corporate Edition на основании параметров реестра и данных, полученных от серверов.
- Выбранный сервер передает клиенту список серверов следующего уровня сетевой иерархии. Navroam просматривает сетевую иерархию до самого низкого уровня. Последний сервер в иерархии становится новым родительским сервером перемещающегося клиента и немедленно передает этому клиенту все параметры конфигурации.
- Navroam запускается регулярно и выполняет следующие проверки:
  - Проверка доступности родительского сервера и его время отклика. Если родительский сервер недоступен или другой родительский сервер может обеспечить более высокую производительность, то Navroam переключает клиента на новый наилучший родительский сервер.
  - Проверка сетевого адреса компьютера. В случае изменения адреса устанавливается соединение с новым наилучшим родительским сервером.
  - Если данный клиент ранее использовал другой родительский сервер, то после установления связи с новым родительским сервером Navroam удалить себя из списка клиентов старого сервера.

Реализация роуминга

Для реализации роуминга выполните следующие действия:

- Проанализируйте сеть Symantec AntiVirus Corporate Edition и составьте ее схему
- В каждой области выделите серверы, которые будут указывать перемещающимся клиентам на следующий уровень серверов роуминга
- Создайте для перемещающихся клиентов список серверов нулевого уровня

■ Создайте список всех серверов роуминга, распределив серверы по уровням иерархии, а при необходимости и по типу (например, сервер изолятора или сервер предупреждений)

■ Настройте поддержку роуминга на перемещающихся клиентах

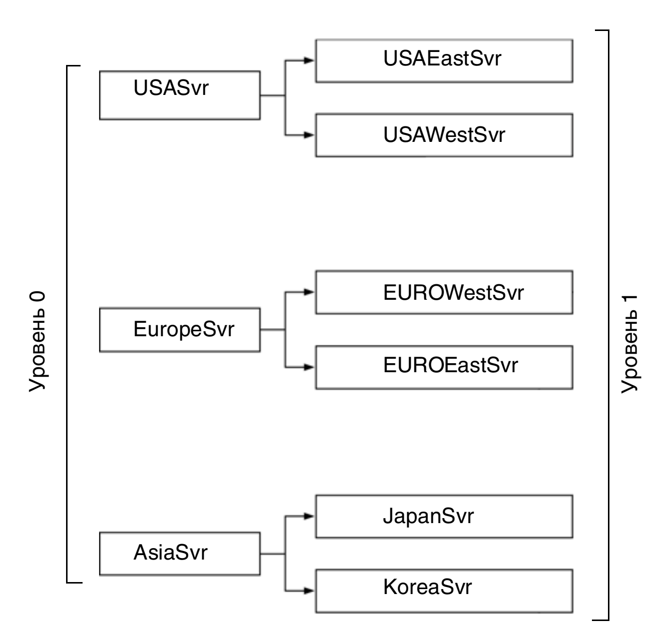
■ Настройте поддержку роуминга на серверах роуминга

Анализ сети Symantec AntiVirus Corporate Edition и составление ее схемы

Несмотря на то, что в сети может применяться множество серверов, не следует настраивать их все в качестве серверов роуминга. Создание иерархической схемы сети позволит вам быстро выбрать серверы роуминга.

На Рис. 6-1 показана схема сети крупного предприятия, работающего на трех континентах. Несмотря на то, что количество серверов Symantec AntiVirus Corporate Edition в организации существенно больше, чем показано на схеме, роль региональных серверов-указателей выполняют только перечисленные серверы.

Рис. 6-1 Пример схемы сети предприятия



Выбор серверов для различных уровней иерархии

При выборе серверов для различных уровней иерархи необходимо проанализировать требования, предъявляемые перемещающимися клиентами. Например, вы можете определить географию перемещения пользователей: заграничные поездки, перемещения в пределах страны или в пределах какого-либо небольшого региона внутри страны. Если пользователь выезжает в другие страны, то его список серверов должен содержать серверы стран нулевого уровня. Если же пользователь перемещается только внутри страны, то в список необходимо включить серверы, начиная с первого уровня.

В зависимости от быстродействия сети, список может содержать только серверы верхнего уровня (для Рис. 6-1 — нулевого уровня). Это упростит создание списка серверов для клиентов. Единственным ограничением количества определяемых уровней является ограничение размера текстового файла 512 знаками.

Создание списка серверов Symantec AntiVirus Corporate Edition нулевого уровня

Для создания списка серверов можно использовать любой текстовый редактор, например, Блокнот. Текстовый файл со списком серверов должен содержать строки в следующем формате:

<local><тип сервера><уровень><список серверов>

где:

- <local> указывает клиенту, что это нулевой уровень серверов, к которым клиент должен пытаться подключиться при поиске сервера роуминга.
- <тип сервера> задает тип данного сервера (например, родительский сервер, сервер изолятора, сервер Grc.dat или сервер предупреждений).
- <уровень> равен 0.
- <список серверов> содержит перечень имен серверов, разделенных запятыми. (Между запятыми можно указывать пробелы.)

Например, список серверов, показанный на Рис. 6-1, будет выглядеть следующим образом:

<local> Parent 0 USASvr,EuropeSvr,AsiaSvr

В данном примере это будет единственная строка в списке серверов для перемещающихся клиентов. Список указывает, что клиент должен

обратиться к трем перечисленным серверам и сравнить их время отклика. В зависимости от того, какой сервер покажет лучший результат, клиент продолжит поиск на более низких уровнях иерархии для выбранного континента.

Создание иерархического списка серверов Symantec AntiVirus Corporate Edition

Для создания иерархического списка можно использовать любой текстовый редактор, например, Блокнот. Файл должен содержать строки в следующем формате:

<компьютер> <тип сервера> <уровень> <список серверов>

где:

- <компьютер> задает имя хоста сервера
- <тип сервера> задает тип данного сервера (например, родительский сервер, сервер изолятора, сервер Grc.dat или сервер предупреждений)
- <уровень> задает уровень, указанный в текстовом файле со списком серверов
- <список серверов> содержит перечень имен серверов, разделенных запятыми (между запятыми можно указывать пробелы)

Например, в организации, описанной на Рис. 6-1, для клиентов в США может применяться следующий список серверов:

USASvr Parent 1 USWestServer,USEastServer

Настройка поддержки роуминга на перемещающихся клиентах

Настройка поддержки роуминга на перемещающихся клиентах включает выполнение следующих задач:

- Включение и настройка роуминга на всех перемещающихся клиентах
- Добавление в реестр всех перемещающихся клиентов сведений о серверах нулевого уровня

Включение и настройка роуминга на всех перемещающихся клиентах

Вы можете включить и настроить поддержку роуминга на клиентах Symantec AntiVirus Corporate Edition путем задания необходимых значений

в файле конфигурации (Grc.dat) или путем прямого редактирования реестра перемещающегося клиента с помощью Regedit. Значения следует задавать в следующем разделе реестра:

HKEY_LOCAL_MACHINE\SOFTWARE\INTEL\LANDesk\VirusProtect6\CurrentVersion\ProductControl

В Табл. 6-2 приведены описания параметров реестра.

Табл. 6-2 Значения реестра для настройки перемещающихся клиентов

Параметр	Описание
ProductControl\RoamClient	1: Включить поддержку перемещающегося клиента (по умолчанию). 0: Выключить поддержку перемещающегося клиента.
ProductControl\RoamQuarantine	1: Включить роуминг центрального изолятора. 0: Выключить роуминг центрального изолятора (по умолчанию).
ProductControl\RoamAlerts	1: Включить роуминг сервера предупреждений. 0: Выключить роуминг сервера предупреждений (по умолчанию).
ProductControl\CheckForNewParentIntervalInSeconds	Интервал проверки нового родительского сервера (в секундах). (По умолчанию задано значение 30 секунд.)
ProductControl\CheckParentIntervalInMinutes	Интервал проверки доступности родительского сервера (в минутах). (По умолчанию задано значение 120 минут.)
ProductControl\SampleCountForParentCheck	Число проверок времени отклика и доступности каждого родительского сервера. Для вычисления окончательного результата все полученные значения усредняются. (По умолчанию задано значение 7.)

Табл. 6-2 Значения реестра для настройки перемещающихся клиентов

Параметр	Описание
ProductControl\FindNearestParent IntervalInMinutes	Интервал проверки на наличие более близкого родительского сервера (в минутах). (По умолчанию задано значение 60 минут.)
ProductControl\RoamManagingParent Level0	Список родительских серверов для проверки расстояния до них.
ProductControl\RoamManagingGRC Level0	Список серверов GRC для проверки расстояния до них.
ProductControl\RoamManaging QuarantineLevel0	Список серверов изолятора для проверки расстояния до них.
ProductControl\RoamManagingAlert Level0	Список серверов предупреждений для проверки расстояния до них.

Информация о применении файлов конфигурации приведена в книге *«Symantec AntiVirus Corporate Edition: Справочник»*.

Добавление в реестр всех перемещающихся клиентов сведений о серверах нулевого уровня

В Symantec AntiVirus Corporate Edition существуют следующие два способа добавления серверов нулевого уровня в реестры перемещающихся клиентов:

- Создайте файл (Grc.dat) с необходимыми параметрами реестра и передайте этот файл на перемещающиеся клиенты.
- С помощью утилиты NAVRoam.exe включите необходимые параметры в реестр перемещающегося клиента. По умолчанию Symantec AntiVirus Corporate Edition копирует утилиту NAVRoam.exe в установочный каталог клиента в процессе установки.

Информация о применении файлов конфигурации приведена в книге *«Symantec AntiVirus Corporate Edition: Справочник»*.

Импорт списка серверов с помощью NAVRoam

1 В каталоге исходных установочных файлов на клиенте Symantec AntiVirus Corporate Edition создайте папку ToNAV и поместите в нее файл со списком серверов.

2 Установите клиента Symantec AntiVirus Corporate Edition.

   В процессе установки содержимое папки ToNAV автоматически копируется в нужную папку.

3 В командной строке перейдите к папке, в которой находится утилита NAVRoam.exe и файл со списком серверов, и введите следующую команду:

   NAVRoam /import ServerListFile.txt

   где ServerListFile.txt — это текстовый файл со списком серверов.

См. «Параметры командной строки» на стр. 178.

Настройка поддержки роуминга на серверах роуминга

Настройка роуминга на серверах Symantec AntiVirus Corporate Edition включает выполнение следующих задач:

- Включение роуминга с помощью задания соответствующего параметра реестра на всех серверах роуминга
- Рассылка иерархического списка серверов на все серверы роуминга с помощью утилиты RoamAdmn.exe, находящейся на диске 1 в папке AdmTools.
- Дополнительная настройка распределения нагрузки, резервных и альтернативных серверов Symantec AntiVirus Corporate Edition

Включение роуминга и рассылка иерархического списка серверов

Для включения роуминга необходимо добавить параметр в реестр каждого сервера роуминга и разослать список серверов. Скопируйте RoamAdmn на компьютер, с которого вы будете рассылать иерархический список серверов на серверы роуминга. При запуске RoamAdmn обращается к серверам, указанным в начале каждой строки в иерархическом списке сервера. RoamAdmn добавляет на каждом сервере параметр реестра со списком серверов, относящихся к следующему уровню иерархии. Если сервер оказывается недоступным, то он пропускается.

Включение роуминга

◆ Добавьте следующие параметры реестра типа DWORD:

  HKEY_LOCAL_MACHINE\SOFTWARE\INTEL\LANDesk\VirusProtect6\CurrentVersion\ProductControl\RoamServer

Рассылка иерархических списков серверов

- В командной строке введите следующую команду:

  RoamAdmn /import serverlist.txt

  где «serverlist.txt» представляет имя созданного вами иерархического списка серверов.

Пример сервера роуминга

В организации есть сервер, доступный для всех серверов роуминга. Включите в файл Serverlist.txt следующие строки:

USASvr Parent 1 USAWestSvr,USAEastSvr

EuropeSvr Parent 1 EUROEastSvr,EUROWestSvr

AsiaSvr Parent 1 JapanSvr,KoreaSvr

В Табл. 6-3 описаны данные файла Serverlist.txt, заносимые в реестр каждого сервера роуминга.

Табл. 6-3 Примеры значений параметров реестра

Имя сервера	Параметр реестра	Значение
USASvr	RoamManagingParentLevel1	USAWestSvr,USAEastSvr
EuropeSvr	RoamManagingParentLevel1	EUROEastSvr,EUROWestSvr
AsiaSvr	RoamManagingParentLevel1	JapanSvr,KoreaSvr

Настройка параметров перемещающихся клиентов

В Табл. 6-4 перечислены параметры перемещающихся клиентов.

Табл. 6-4 Параметры перемещающихся клиентов

Параметр	Описание
Выравнивание нагрузки	Если при наличии нескольких серверов вы хотите равномерно распределить перемещающихся клиентов между ними, то вы можете выровнять нагрузку на серверы, указав, что клиенты должны считать все серверы равными, независимо от времени отклика того или иного сервера. Перемещающийся клиент будет опрашивать все серверы списка. Серверы роуминга отслеживают количество обслуживаемых ими клиентов Symantec AntiVirus Corporate Edition и сообщают это значение перемещающемуся клиенту. Клиент выбирает сервер с минимальным количеством клиентов. Этот сервер будет новым родительским сервером перемещающегося клиента. Параметр выравнивания нагрузки имеет более высокий приоритет, чем поиск ближайшего родительского сервера.
Резервные серверы	Вы можете указать резервные серверы для обработки запросов клиентов в случае недоступности серверов роуминга. Перемещающийся клиент проверяет время ответа первого ответившего сервера, указанного в списке. Если первый резервный сервер становится недоступным, то после проверки доступа к родительскому серверу управляемые им перемещающиеся клиенты переключатся на следующий указанный в списке резервный сервер. Резервные серверы не поддерживают выравнивание нагрузки.
Альтернативные серверы	Помимо родительских серверов вы также можете настроить для перемещающихся клиентов подключение к серверу центрального изолятора (на котором также должен быть установлен сервер Symantec AntiVirus Corporate Edition), серверу предупреждений (AMS^2) и к серверу Grc.dat. Последний сервер предоставляет перемещающимся клиентам файл настройки Grc.dat. Применение nearest_GRC позволяет указать, что перемещающийся клиент должен получать параметры политики с указанного сервера и немедленно их обрабатывать. **Примечание:** Клиент не может подключаться к нескольким родительским серверам одного типа.

Настройка параметров перемещающихся клиентов

Вы можете настроить параметры перемещающихся клиентов, включив выравнивание нагрузки, задав резервные серверы, и разрешив подключение к серверам других типов.

Настройка выравнивания нагрузки на серверы

- Укажите между именами серверов в иерархическом списке знак равенства (=).

  Например:

  SouthEastSvr Parent 4 MiamiSvr=AtlantaSvr=RichmondSvr

Настройка резервного сервера

- Укажите в иерархическом списке серверов символ «больше» (>).

  Например:

  SouthEastSvr Parent 4 MiamiSvr>AtlantaSvr>RichmondSvr

Включение подключения к серверам других типов

1. На перемещающихся клиентах присвойте параметру реестра, задающему тип сервера, значение 1.

   См. «Параметры реестра» на стр. 180.

2. Введите в командной строке любую из следующих команд:

   NAVRoam /nearest_parent

   NAVRoam /nearest_quarantine

   NAVRoam /nearest_GRC

   NAVRoam /nearest_alerts

   Основное отличие между /nearest_parent и /nearest_GRC проявляется при обработке файла конфигурации (Grc.dat). Применение /nearest_parent указывает, что перемещающийся клиент должен найти ближайший родительский сервер. Параметры политики не обрабатываются до тех пор, пока клиент не подключится к родительскому серверу. Применение /nearest_GRC позволяет перемещающимся клиентам немедленно получать с родительского сервера параметры политики и обрабатывать их.

Параметры командной строки

В Табл. 6-5 описаны параметры командной строки, которые могут применяться с утилитами NAVRoam.exe и RoamAdmn.exe.

Для применения параметров командной строки необходимы права доступа администратора.

Табл. 6-5 Параметры командной строки

Параметр	Описание
/h	Отображение списка параметров с описанием их применения.
/import <список серверов>	Настройка разделов реестра сервера или клиента. С помощью программы RoamAdmn.exe можно импортировать список серверов на удаленные серверы. С помощью программы NAVRoam.exe можно импортировать список серверов в реестр локального компьютера. <список серверов> — это текстовый файл, в котором содержится список возможных родительских серверов.
/export <файл>	Вывод списка всех серверов роуминга, которые клиент может найти на всех уровнях для всех типов родительских серверов (родительский сервер, сервер изолятора, сервер предупреждений и сервер Grc.dat). <файл> — это имя файла, в котором записаны необходимые данные. Файл, созданный с помощью команды экспорта, можно использовать в качестве списка серверов для импорта.
/install <путь> <имя новой службы> <имя нового исполняемого файла>	Регистрирует и запускает службу перемещающегося клиента. Служба будет работать до тех пор, пока компьютер не будет выключен. <путь> задает путь к папке, в которую требуется скопировать программу NAVRoam.exe. <имя нового исполняемого файла> — это имя NAVRoam.exe. <имя нового исполняемого файла> — это имя NAVRoam.exe.
/remove <имя новой службы>	Остановка и удаление NAVRoam.exe.

Табл. 6-5 Параметры командной строки

Параметр	Описание
/nearest	Поиск и назначение ближайшего подходящего родительского сервера, сервера изолятора, сервера предупреждений или сервера Grc.dat. Необходимо, чтобы путь GRC родительского сервера был вручную задан в реестре.
/nearest_parent	Поиск и назначение ближайшего к клиенту родительского сервера.
/nearest_quarantine	Поиск и назначение ближайшего к клиенту родительского сервера Изолятора.
/nearest_GRC	Поиск и применение файла конфигурации (Grc.dat) с ближайшего сервера Grc.dat. Необходимо, чтобы путь GRC родительского сервера был вручную задан в реестре.
/nearest_alerts	Поиск и назначение ближайшего сервера предупреждений (AMS[2]).
/check_parent	Проверка доступности родительского сервера.
/shutdown	Отключение клиента от родительского сервера.
/time-network <затраченное-время-в-секундах> <время-паузы-в-миллисекундах> <серверы>	Вывод информации о среднем промежутке времени, необходимом для установления связи с каждым из указанных серверов. <затраченное-время-в-секундах> указывает, сколько должно занять выполнение процесса. <время-паузы-в-миллисекундах> указывает частоту обращения к серверу. Например, при установке значения 10 000 клиент будет обращаться к серверу каждые десять секунд. <серверы> — список проверяемых серверов. Имена серверов разделяются запятыми. Не включайте пробелы между именами серверов и запятыми.

Параметры реестра

Вы можете изменять значения параметров реестров, управляющих роумингом, с помощью редактора реестра, например, Regedit или Regedt32.

Поведением агента управляют параметры реестра, находящиеся в следующем разделе:

HKEY_LOCAL_MACHINE\SOFTWARE\INTEL\LANDesk\VirusProtect6\CurrentVersion\ProductControl

В Табл. 6-6 описаны параметры реестра, управляющие перемещающимися клиентами.

Табл. 6-6 Параметры реестра для перемещающихся клиентов

Параметр реестра	Описание
CheckForNewParentIntervalInSeconds	Если компьютер не может найти ближайший родительский сервер при первом запуске, он периодически проверяет, работает ли сеть. Периодичность проверки задается с помощью этого параметра. По умолчанию задано значение 30 секунд.
CheckParentIntervalInMinutes	Этот параметр определяет, как часто компьютер проверяет доступность своего родительского сервера. Если родительский сервер недоступен, то предпринимается попытка найти новый родительский сервер. По умолчанию задано значение 120 минут.
RoamClient	Этот параметр дает указание агенту сделать этот компьютер дочерним для ближайшего родительского сервера. Установите значение 0, если данный компьютер не должен становиться дочерним компьютером ближайшего родительского сервера.
RoamQuarantine	Если установлено значение 1, то пересылка в изолятор осуществляется на ближайший сервер, найденный в параметрах поиска изолятора. По умолчанию задано значение 0.

Табл. 6-6 Параметры реестра для перемещающихся клиентов

Параметр реестра	Описание
RoamAlerts	Если установлено значение 1, то пересылка предупреждений AMS[2] осуществляется на ближайший сервер, найденный в параметрах поиска серверов предупреждений. По умолчанию задано значение 0.
RoamGRC	Если задано значение 1, то клиент подключается к серверу, с которого от должен получать обновления файла конфигурации (Grc.dat). По умолчанию задано значение 0.
RoamServer	Если установлено значение 1, то клиент подключается к наилучшему родительскому серверу. По умолчанию задано значение 0.
ParentGRCPath	Присваивает параметру ParentGRCPath значение файла конфигурации (Grc.dat). Агент копирует файл конфигурации на локальный компьютер и применяет его. См. приведенное выше описание RoamGRC. Если параметрам RoamClient и RoamGRC присвоено значение 1, то NAVRoam.exe копирует файлы конфигурации с родительского сервера, а затем копирует файлы конфигурации с родительского сервера GRC и заменяет копию файла, полученную с родительского сервера.
ParentLiveUpdateHstPath	Определяет каталог в основном каталоге NAV, например, \Myliveupdatehost\Liveupdt.hst Файл .hst должен находиться в OSDRIVE/ ProgramFiles/Symantec/LiveUpdate. В этот каталог агент копирует полученный с хоста файл LiveUpdate.

Глава 7

Работа с журналами

Эта глава содержит следующие разделы:

Сведения о журналах

Журналы позволяют централизованно получать информацию об обнаруженных вирусах и об осмотрах, выполняемых в сети. С помощью Symantec System Center вы можете выполнять следующие операции:

- Просматривать данные на уровне группы серверов, отдельного сервера или на уровне управляемой рабочей станции. Кроме того, на каждом клиенте Symantec AntiVirus Corporate Edition хранится локальная копия собственного журнала событий. Данные можно просматривать с помощью пользовательского интерфейса клиента Symantec AntiVirus Corporate Edition.
- Сортировать и фильтровать записи журналов.
- Выполнять различные действия на основании данных из записей журналов. Например, если в журнале вирусов есть запись об обнаружении вируса, то вы можете выполнить определенное действие, например, удалить вирус или переместить зараженный файл в центральный изолятор.
- Экспортировать данные в файл Microsoft Access (в формате .mdb) или в файл с разделителями-запятыми (CSV).
- Удалять данные журналов.

Symantec AntiVirus Corporate Edition поддерживает следующие типы журналов, описанные в Табл. 7-1.

Табл. 7-1 Типы журналов

Имя	**Описание**	**Объекты, для которых ведутся журналы**
Журнал событий	Содержит информацию о запуске и завершении работы Symantec AntiVirus Corporate Edition, информацию о запущенных, остановленных и прерванных осмотрах, об изменениях конфигурации, обновлениях файлов описаний вирусов, о заражении вирусами, а также сведения об объектах, переданных в центральный изолятор и в центр Symantec Security Response.	■ Группы серверов ■ Отдельные серверы ■ Отдельные клиенты

Табл. 7-1 Типы журналов

Имя	Описание	Объекты, для которых ведутся журналы
Журнал осмотров	Содержит информацию об осмотрах, выполненных или работающих на клиентах Symantec AntiVirus Corporate Edition на уровне группы серверов, отдельного сервера или рабочей станции. Имеется возможность указать промежуток времени для отбора элементов журнала. Например, можно просмотреть сведения только об осмотрах, выполненных за последние семь дней.	■ Группы серверов ■ Отдельные серверы ■ Отдельные клиенты
Журнал вирусов	В этом журнале перечислены все вирусы, обнаруженные на выбранных компьютерах или группах серверов. Выбрав объект в списке, можно применить к нему дополнительные действия, например, удалить или изолировать. В журнале вирусов представлены подробные сведения о каждом случае заражения, например, имя и местонахождения зараженного файла, имя зараженного компьютера, первичное и вторичное действия, предусмотренные на случай обнаружения вируса, а также сведения о том, какое действие было выполнено.	■ Группы серверов ■ Отдельные серверы ■ Отдельные клиенты
Журнал сплошных проверок	Содержит информацию о сплошных проверках серверов и групп серверов.	■ Группы серверов ■ Отдельные серверы

Сортировка и фильтрация записей журналов

При просмотре журналов имеется возможность просматривать только элементы, относящиеся к определенным датам. Эта функция относится к журналу вирусов, журналу сплошных проверок, журналу осмотров и журналу событий. Можно выбрать следующие диапазоны дат:

- Сегодня
- Последние 7 дней
- Текущий месяц

- Все элементы
- Выбранный диапазон дат

Вы также можете фильтровать список событий, включая в него лишь интересующие вас события.

Сортировка и фильтрация записей журналов

При работе с журналом вирусов, журналами осмотров и с журналом событий можно сортировать данные по значениям любого столбца.

При работе с этими журналами можно фильтровать записи по дате. При работе с журналом событий возможна также фильтрация по типу события.

Сортировка данных

- ◆ Щелкните на заголовке столбца

  При первом щелчке в заголовке столбца появится значок сортировки по возрастанию. При втором щелчке в заголовке столбца появится значок сортировки по убыванию.

Фильтрация записей журналов по дате

1. В окне консоли Symantec System Center щелкните правой кнопкой мыши на сервере или группе серверов, затем выберите команды **Все задачи** > **Symantec AntiVirus** > **Журналы**, а затем выберите один из следующих вариантов:
   - Журнал событий
   - Журнал осмотров
   - Журнал вирусов
   - Журнал сплошных проверок
2. Выберите в списке одно из следующих значений:
   - Сегодня
   - Последние 7 дней
   - Текущий месяц
   - Все элементы
   - Диапазон

     Если был выбран **Диапазон**, то укажите начальную и конечную даты и нажмите кнопку **OK**.

Фильтрация данных журнала событий по типу событий

1. В окне консоли Symantec System Center щелкните правой кнопкой мыши на сервере или группе серверов, и выберите команды **Все задачи** > **Symantec AntiVirus** > **Журналы** > **Журнал событий**.
2. В окне журнала событий щелкните на значке фильтра.
3. В окне фильтра журнала событий выберите события, которые должны быть включены в список.
   - Изменение конфигурации
   - Запуск и завершение работы Norton AntiVirus
   - Файл описаний вирусов
   - Пропуск осмотра
   - Отправка объекта на сервер изолятора
   - Доставка объекта в центр Symantec Security Response
4. Нажмите кнопку **OK**.

Просмотр журналов

В Табл. 7-2 описаны журналы, которые можно просмотреть с помощью консоли Symantec System Center.

Табл. 7-2 Журналы

Журнал	Описание
Журнал вирусов	■ На уровне группы серверов позволяет просмотреть информацию о всех вирусах, найденных в этой группе. ■ На уровне сервера позволяет просмотреть информацию о всех вирусах, найденных на клиентах, управляемых этим сервером. ■ На уровне клиента позволяет просмотреть информацию о всех вирусах, найденных на этом клиенте.
Журнал сплошных проверок	■ На уровне группы серверов и на уровне сервера позволяет просмотреть информацию о всех сплошных проверках на данном сервере или на всех серверах группы.
Журнал осмотров (текущих и плановых)	■ На уровне группы серверов позволяет просмотреть информацию о всех осмотрах, выполненных в этой группе. ■ На уровне сервера позволяет просмотреть информацию о всех сплошных проверках, выполненных на клиентах, управляемых этим сервером. ■ На уровне клиента позволяет просмотреть информацию о всех сплошных проверках, выполненных на этом клиенте.

Просмотр журналов

Вы можете просмотреть журнал вирусов, журнал сплошных проверок и журнал осмотров.

См. «Работа с журналом вирусов» на стр. 189.

Просмотр журнала вирусов

◆ В окне консоли Symantec System Center щелкните правой кнопкой мыши на группе серверов, сервере или отдельном клиенте, и выберите команды **Все задачи** > **Symantec AntiVirus** > **Журналы** > **Журнал вирусов**.

См. «Информация о значках журнала событий» на стр. 194.

Просмотр журнала сплошных проверок

1. В окне консоли Symantec System Center щелкните правой кнопкой мыши на сервере или группе серверов, и выберите команды **Все задачи** > **Symantec AntiVirus** > **Журналы** > **Журнал сплошных осмотров**.
2. В окне журнала сплошных осмотров нажмите кнопку **Просмотр результатов** для просмотра результатов сплошных проверок.

Просмотр журнала осмотров

- В окне консоли Symantec System Center щелкните правой кнопкой мыши на группе серверов или на отдельном клиенте, и выберите команды **Все задачи** > **Symantec AntiVirus** > **Журналы** > **Журнал осмотров**.

Работа с журналом вирусов

В окне журнала вирусов показаны значки с информацией о найденных вирусах. С помощью этого окна вы также можете выполнять различные действия, например, сохранять файлы в формате CSV.

Примечание: Нельзя применить дополнительные действия к данным электронной почты. Для сжатых файлов можно выполнить лишь ограниченный набор действий.

В Табл. 7-3 приведено описание значков журнала вирусов.

Табл. 7-3 Значки журнала вирусов

Значок	Описание
	Файл заражен.
	Файл не заражен. Файл не был заражен, либо был успешно исправлен. Для получения более подробных сведений просмотрите действия, примененные к файлу.
	Произошла ошибка, связанная с этим файлом.
	Закрыть окно журнала вирусов.

В Табл. 7-4 приведены описания действий, которые можно выполнить с помощью окна журнала вирусов.

Табл. 7-4 Действия журнала вирусов

Действие	Описание
Отменить действие	Symantec AntiVirus Corporate Edition позволяет отменить последнее действие, выполненное над зараженным файлом, включая удаление этого файла из изолятора и удаление расширения .vbn у переименованного файла. Symantec AntiVirus Corporate Edition не может восстановить удаленный файл. Отменить действия, примененные к сжатым файлам, нельзя.
Исправить	Файлы описаний вирусов Symantec AntiVirus Corporate Edition обновляются очень часто. Файл, который не удалось исправить вчера или несколько недель назад, может быть исправлен после обновления описаний вирусов. Применить это действие к сжатым файлам нельзя.
Удалить файл	Вы можете удалить любой зараженный файл (в том числе сжатый), который хранится в изоляторе или журнале вирусов. Удаленные файлы восстановить нельзя.
Изолировать	Если вы определили, что Symantec AntiVirus Corporate Edition оставил зараженный файл без изменений, то такой файл следует переместить в изолятор, чтобы вирус не мог распространяться. Сжатые файлы также можно переместить в изолятор.
Экспортировать	Вы можете экспортировать информацию о выбранном объекте журнала вирусов или журнала событий в файл CSV или в базу данных Microsoft Access.

Работа с журналом вирусов

Журнал вирусов позволяет отменить последнее действие, выполненное над файлом, исправить файл, удалить его, либо переместить файл в центральный изолятор. Вы также можете экспортировать данные журнала вирусов.

Отмена последнего выполненного действия

1 Щелкните на файле правой кнопкой мыши и выберите команду **Отменить действие**.

2 В окне действий нажмите кнопку **Вернуть**.

Исправление зараженного файла

1 Щелкните на файле правой кнопкой мыши и выберите команду **Исправить**.

2 В окне действий нажмите кнопку **Исправить**.

Удаление зараженного файла

1 Щелкните на файле правой кнопкой мыши и выберите команду **Удалить**.

2 В окне действий нажмите кнопку **Удалить**.
Удаленные файлы восстановить нельзя.

Перемещение файлов в центральный изолятор

1 Щелкните на файле правой кнопкой мыши и выберите команду **Изолировать**.

2 В окне действий нажмите кнопку **Изолировать**.

Экспорт данных журнала вирусов

1 Щелкните на файле правой кнопкой мыши и выберите команду **Экспорт**.

2 В списке типов сохраняемых файлов выберите одно из следующих значений:

- CSV
- База данных Access

3 В поле имени файла укажите имя.

4 Нажмите кнопку **OK**.

Работа с журналом осмотров

В окне журнала осмотров показаны значки с информацией о найденных вирусах. С помощью этого окна вы также можете выполнять различные действия, например, сохранять данные в формате CSV.

Примечание: Действия над данными электронной почты производить нельзя, а к сжатым файлам применяется ограниченный набор действий.

В Табл. 7-5 приведено описание значков.

Табл. 7-5 Значки журнала осмотров

Значок	Описание
	Файл заражен.
	Файл не заражен. Файл не был заражен, либо был успешно исправлен. Для просмотра более подробных сведений просмотрите действия, примененные к файлу.
	Закрыть окно журнала осмотров.
	Просмотр свойств объекта.
	Сохранение данных журнала осмотров в файле в формате списка с разделителями-запятыми (.csv).
	Отображение справочной информации о журнале осмотров.

В Табл. 7-6 приведены описания действий, которые можно выполнить с помощью окна журнала осмотров.

Табл. 7-6 Действия журнала осмотров

Действие	Описание
Отменить действие	Symantec AntiVirus Corporate Edition позволяет отменить последнее действие, выполненное над зараженным файлом, включая удаление этого файла из изолятора и удаление расширения .vbn у переименованного файла. Symantec AntiVirus Corporate Edition не может восстановить удаленный файл. Отменить действия, примененные к сжатым файлам, нельзя.
Исправить	Файлы описаний вирусов Symantec AntiVirus Corporate Edition обновляются очень часто. Файл, который не удалось ранее, может быть исправлен после обновления описаний вирусов. Применить это действие к сжатым файлам нельзя.
Удалить файл	Вы можете удалить любой зараженный файл (в том числе сжатый), который хранится в изоляторе или журнале осмотров. Удаленные файлы восстановить нельзя.

Табл. 7-6 Действия журнала осмотров

Действие	Описание
Изолировать	Если вы определили, что Symantec AntiVirus Corporate Edition оставил зараженный файл без изменений, то такой файл следует переместить в изолятор, чтобы вирус не мог распространяться. Сжатые файлы также можно переместить в изолятор.
Экспорт	Вы можете экспортировать информацию о выбранном объекте журнала осмотров или журнала событий в файл CSV или в базу данных Microsoft Access.

Работа с журналом осмотров

Журнал осмотров позволяет отменить последнее действие, выполненное над файлом, исправить файл, удалить его, либо переместить файл в центральный изолятор. Вы также можете экспортировать данные журнала осмотров.

Отмена последнего выполненного действия

1. Щелкните на файле правой кнопкой мыши и выберите команду **Отменить действие**.
2. В окне действий нажмите кнопку **Вернуть**.

Исправление зараженного файла

1. Щелкните на файле правой кнопкой мыши и выберите команду **Исправить**.
2. В окне действий нажмите кнопку **Исправить**.

Удаление зараженного файла

1. Щелкните на файле правой кнопкой мыши и выберите команду **Удалить**.
2. В окне действий нажмите кнопку **Удалить**.
   Удаленные файлы восстановить нельзя.

Перемещение файлов в центральный изолятор

1. Щелкните на файле правой кнопкой мыши и выберите команду **Изолировать**.
2. В окне действий нажмите кнопку **Изолировать**.

Экспорт данных журнала осмотров

1. Щелкните на файле правой кнопкой мыши и выберите команду **Экспорт**.
2. В списке типов сохраняемых файлов выберите одно из следующих значений:
   - CSV
   - База данных Access
3. В поле имени файла укажите имя.
4. Нажмите кнопку **OK**.

Информация о значках журнала событий

В окне журнала событий с помощью значков отображается информация о найденных вирусов. С помощью этого окна вы также можете выполнять различные действия, например, сохранять данные в файле CSV.

В Табл. 7-7 приведено описание значков.

Табл. 7-7 Значки журнала событий

Значок	Описание
	Получить информацию о событии.
	Произошла ошибка, связанная с этим событием.
	Закрыть окно журнала событий.
	Просмотр свойств объекта.
	Сохранить данные журнала событий в файле CSV или в файле базы данных Microsoft Access.
	Отфильтровать записи журнала событий по следующим категориям: ■ Изменение конфигурации ■ Запуск или завершение работы Symantec AntiVirus Corporate Edition ■ Файл описаний вирусов ■ Пропуск осмотра ■ Пересылка объекта в изолятор ■ Доставка объекта в центр Symantec Security Response
	Просмотреть справочную информацию о журнале событий.

Удаление записей из журналов

Вы можете настроить Symantec AntiVirus Corporate Edition таким образом, чтобы из журналов автоматически удалялись данные, хранящиеся в них дольше определенного времени.

Настройка частоты удаления

1. В консоли Symantec System Center щелкните правой кнопкой мыши на группе серверов, отдельном сервере или клиенте, и выберите команды **Все задачи** > **Symantec AntiVirus** > **Настройка журналов**.
2. В окне параметров журналов выберите интервал времени, по истечение которого записи должны удаляться из журналов.
3. Нажмите кнопку **OK**.

   Эта операция не удаляет данные, а только скрывает их при просмотре журналов. Чтобы полностью удалить записи журнала, необходимо удалить файлы с расширением .log, содержащие записи событий. События заносятся в файлы .log, хранящиеся в каталоге Logs, по одному файлу для каждого дня недели. Имена этим файлам присваиваются в соответствии с днем их создания.

Алфавитный указатель

З

И

К

Л

М

Н

О

П

Р

С

У

Ф

Э

G

I

L

S

Обслуживание и техническая поддержка

Компания Symantec стремится обеспечивать высокое качество обслуживания клиентов во всем мире. Она предоставляет помощь профессионалов в любой точке мира для решения вопросов, связанных с применением программного обеспечения и услуг.

Порядок обслуживания клиентов и технической поддержки в разных странах различен.

Если у вас возникнут вопросы относительно описанных ниже услуг, обратитесь к разделу «Центры обслуживания клиентов и технической поддержки».

Регистрация и лицензии

Если для работы с продуктом необходима регистрация или код лицензии, рекомендуем вам обратиться на Web-сайт регистрации и лицензирования фирмы Symantec, расположенный по адресу www.symantec.com/certificate. Кроме того, можно обратиться по адресу http://www.symantec.com/techsupp/ent/enterprise.html, выбрать программный продукт, который необходимо зарегистрировать, и воспользоваться соответствующей ссылкой для лицензирования и регистрации на домашней странице этого продукта.

Если вы приобрели подписку на техническую поддержку, то для решения технических вопросов можно обратиться в компанию Symantec по телефону или через Интернет. При первом обращении в службу технической поддержки будьте готовы назвать номер вашего лицензионного сертификата или контактный идентификатор, полученный при регистрации продукта, чтобы сотрудники службы поддержки могли

проверить ваше право на получение соответствующей услуги. Если вы не приобрели подписку на техническую поддержку, то для получения подробных сведений о предоставляемых услугах технической поддержки обратитесь в отдел обслуживания клиентов фирмы Symantec или по месту приобретения продукта.

Обновление средств защиты

Самые последние сведения о вирусах и потенциальных угрозах можно получить на Web-сайте Symantec Security Response (ранее называвшемся Центром антивирусных исследований – Antivirus Research Center) по адресу:

http://securityresponse.symantec.com

На этом сайте представлены обширные сведения по вопросам обеспечения безопасности и о вирусных угрозах, а также новейшие файлы описаний вирусов. Описания вирусов также можно загрузить с помощью функции LiveUpdate, входящей в состав программных продуктов.

Продление подписки на получение антивирусных обновлений

Приобретение вместе с программным продуктом пакета услуг по его обслуживанию позволяет загружать бесплатные обновления описаний вирусов на протяжении срока действия договора об обслуживании. Если срок действия договора об обслуживании закончился, обратитесь по месту приобретения продукта или в отдел обслуживания клиентов компании Symantec за информацией об условиях продления договора об обслуживании.

Web-сайты компании Symantec

Домашняя страница Symantec на различных языках

На английском языке:	http://www.symantec.com
На русском языке:	http://www.symantec.ru
На французском языке:	http://www.symantec.fr
На немецком языке:	http://www.symantec.de
На итальянском языке:	http://www.symantec.it
На голландском языке:	http:// www.symantec.nl

Symantec Security Response

http://securityresponse.symantec.com

Страница Symantec Enterprise Service and Support

http://www.symantec.com/techsupp/bizsolutions/

Бюллетени новостей для отдельных продуктов

США и Азиатско-Тихоокеанский регион, на английском языке:

http://www.symantec.com/techsupp/bulletin/index.html

Европа, Ближний Восток и Африка, на английском языке:

http://www.symantec.com/region/reg_eu/techsupp/bulletin/index.html

На французском языке:

http://www.symantec.com/region/fr/techsupp/bulletin/index.html.

На немецком языке:

http://www.symantec.com/region/de/techsupp/bulletin/index.html

На голландском языке:

http://www.symantec.com/region/nl/techsupp/bulletin/index.html

На итальянском языке:

http://www.symantec.com/region/it/techsupp/bulletin/index.html

Техническая поддержка

Являясь составной частью центра Symantec Security Response, наша группа глобальной технической поддержки обеспечивает работу центров поддержки по всему миру. Нашей основной деятельностью являются ответы на вопросы о функциях и программных продуктах, их установке и настройке, а также пополнение базы знаний, доступной через Интернет. Мы работаем в тесном сотрудничестве с другими подразделениями компании Symantec, что позволяет отвечать на ваши вопросы в кратчайшие сроки. Например, мы сотрудничаем с отделом разработки продуктов и с антивирусными исследовательскими центрами для обеспечения работы служб оповещения и обновления описаний вирусов в случае распространения новых вирусов и для рассылки оповещений. Мы предлагаем следующие услуги:

- Различные варианты поддержки, позволяющие выбрать набор необходимых услуг для организации любого размера;
- Предоставление поддержки по телефону и через Интернет, что позволяет найти решение в кратчайшие сроки и получить самую свежую информацию;
- Обновления программных продуктов, позволяющие автоматически обновлять средства защиты;
- Обновления сигнатур и описаний вирусов, обеспечивающие высокий уровень безопасности;
- Глобальная поддержка с участием специалистов центра Symantec Security Response, доступная ежедневно и круглосуточно по всему миру на нескольких языках;
- Дополнительные функции, такие как служба оповещения Symantec и возможность назначения менеджера по техническим вопросам, расширяющие возможности для получения эффективной и профессиональной поддержки.

Сведения о предлагаемых в настоящее время программах поддержки можно получить на нашем Web-сайте.

Что необходимо для обращения в службу поддержки

Пользователи, заключившие договор о технической поддержке, могут обращаться в службу технической поддержки по телефону или через Интернет по следующему адресу или по адресу одного из указанных ниже Web-сайтов региональной службы поддержки.

www.symantec.com/techsupp/ent/enterprise.html

При обращении в службу поддержки вам потребуется сообщить следующую информацию:

- Номер версии программного продукта
- Сведения об аппаратном обеспечении
- Объем оперативной памяти, емкость диска, сведения о сетевом адаптере
- Сведения об операционной системе
- Номер версии и пакета обновления
- Топология сети
- Сведения о маршрутизаторе, шлюзе и IP-адресах
- Описание возникших неполадок
- Сообщения об ошибках, файлы журналов
- Действия по устранению неполадок, выполненные перед обращением в компанию Symantec
- Сведения об изменениях, недавно внесенных в конфигурацию программного обеспечения или сети

Обслуживание клиентов

В Центре обслуживания клиентов компании Symantec можно получить сведения по вопросам, не связанным с технической поддержкой, например:

- Общие сведения о продукте (например, основные функции, поддерживаемые языки, торговые представительства в вашем регионе и т.д.)
- Основные методы устранения неполадок, например, как узнать версию продукта
- Последние данные об обновлениях программного продукта

- Инструкции по обновлению и модернизации программного продукта
- Инструкции по регистрации программного продукта или лицензии
- Сведения о программах лицензирования компании Symantec
- Информация о контрактах на льготное обновление и обслуживание
- Замена компакт-дисков и руководств
- Обновление регистрационных данных в связи с изменением адреса или имени владельца программного продукта
- Описание различных вариантов технической поддержки, предлагаемых компанией Symantec

Подробные сведения об обслуживании клиентов можно получить на Web-сайте обслуживания и поддержки компании Symantec, а также в центре обслуживания клиентов компании Symantec. Номера телефонов и адреса Web-сайтов центра обслуживания клиентов, расположенного в вашем регионе, можно найти в разделе «Центры обслуживания клиентов и технической поддержки», приведенном в конце главы.

Центры обслуживания клиентов и технической поддержки

Европа, Ближний Восток и Африка

Web-сайты обслуживания и технической поддержки компании Symantec

На английском языке:	www.symantec.com/eusupport/
На французском языке:	www.symantec.fr/frsupport
На немецком языке:	www.symantec.de/desupport/
На итальянском языке:	www.symantec.it/itsupport/
На голландском языке:	www.symantec.nl/nlsupport/
FTP-сайт компании Symantec: (Загрузка сведений по техническим вопросам и последних пакетов обновлений)	ftp.symantec.com

Посетите Web-сайты обслуживания и технической поддержки компании Symantec, на которых можно найти технические и общие сведения о различных программных продуктах.

Symantec Security Response

http://securityresponse.symantec.com

Бюллетени новостей для отдельных продуктов

США, на английском языке:

http://www.symantec.com/techsupp/bulletin/index.html

Европа, Ближний Восток и Африка, на английском языке:

http://www.symantec.com/region/reg_eu/techsupp/bulletin/index.html

На французском языке:

http://www.symantec.com/region/fr/techsupp/bulletin/index.html

На немецком языке:

http://www.symantec.com/region/de/techsupp/bulletin/index.html

На голландском языке:

http://www.symantec.com/region/nl/techsupp/bulletin/index.html

На итальянском языке:

http://www.symantec.com/region/it/techsupp/bulletin/index.html

Отдел обслуживания клиентов компании Symantec

Для получения информации, не касающейся технических вопросов, и рекомендаций по выполнению ряда задач можно обратиться по указанным ниже телефонам на одном из следующих языков: английском, немецком, французском или итальянском:

Австрия	+ (43) 1 50 137 5030
Бельгия	+ (32) 2 2750173
Великобритания	+ (44) 20 7744 0367
Германия	+ (49) 69 6641 0315
Дания	+ (45) 35 44 57 04
Ирландия	+ (353) 1 811 8093
Испания	+ (34) 91 7456467
Италия	+ (39) 02 48270040
Люксембург	+ (352) 29 84 79 50 30
Нидерланды	+ (31) 20 5040698

Норвегия	+ (47) 23 05 33 05
Финляндия	+ (358) 9 22 906003
Франция	+ (33) 1 70 20 00 00
Швеция	+ (46) 8 579 29007
Швейцария	+ (41) 2 23110001
ЮАР	+ (27) 11 797 6639
Прочие страны (только на английском языке)	+ (353) 1 811 8093

Почтовый адрес отдела обслуживания клиентов компании Symantec

Symantec Ltd
Customer Service Centre
Europe, Middle East and Africa (EMEA)
PO Box 5689
Dublin 15
Ireland

Сведения для клиентов из Азиатско-Тихоокеанского региона

Компания Symantec обеспечивает техническую поддержку и обслуживание клиентов по всему миру. В различных странах обслуживание клиентов организовано по-разному. В частности, в некоторых регионах нет представительства компании Symantec, и указанные услуги предоставляются международными партнерами Symantec. Для получения общей информации обратитесь в региональный отдел обслуживания и поддержки компании Symantec.

Отделы обслуживания клиентов и технической поддержки

Австралия

Symantec Australia
Level 2, 1 Julius Avenue
North Ryde, NSW 2113
Australia

Основной номер телефона	+61 2 8879 1000	
Факс	+61 2 8879 1001	
Web-сайт	http://service.symantec.com	
Техническая поддержка по плану Gold	1800 805 834	gold.au@symantec.com
Информация о контрактах технической поддержки	1800 808 089	contractsadmin@symantec.com

Гонконг

Symantec Hong Kong
Central Plaza
Suite #3006
30th Floor, 18 Harbour Road
Wanchai
Hong Kong

Основной номер телефона	+852 2528 6206
Техническая поддержка	+852 2528 6206
Факс	+852 2526 2646
Web-сайт	http://www.symantec.com.hk

Индия

Symantec India
Suite #801
Senteck Centrako
MMTC Building
Bandra Kurla Complex
Bandra (East)
Mumbai 400051, India

Основной номер телефона	+91 22 652 0658
Факс	+91 22 652 0671
Web-сайт	http://www.symantec.com/india
Техническая поддержка:	+91 22 657 0669

Китай

Symantec China
Unit 1-4, Level 11,
Tower E3, The Towers, Oriental Plaza
No.1 East Chang An Ave.,
Dong Cheng District
Beijing 100738
China P.R.C.

Основной номер телефона	+86 10 8518 3338
Техническая поддержка	+86 10 8518 6923
Факс	+86 10 8518 6928
Web-сайт	http://www.symantec.com.cn

Корея

Symantec Korea
15,16th Floor
Dukmyung B/D
170-9 Samsung-Dong
KangNam-Gu
Seoul 135-741
South Korea

Основной номер телефона	+822 3420 8600
Факс	+822 3452 1610
Техническая поддержка	+822 3420 8650
Web-сайт	http://www.symantec.co.kr

Малайзия

Symantec Corporation (Malaysia) Sdn Bhd
31-3A Jalan SS23/15
Taman S.E.A.
47400 Petaling Jaya
Selangor Darul Ehsan
Malaysia

Основной номер телефона	+603 7805 4910
Факс	+603 7804 9280
Электронный адрес для юридических лиц	gold.apac@symantec.com
Номер телефона для бесплатных звонков	1800 805 104
Web-сайт	http://www.symantec.com.my

Новая Зеландия

Symantec New Zealand
Level 5, University of Otago Building
385 Queen Street
Auckland Central 1001
New Zealand

Основной номер телефона	+64 9 375 4100	
Факс	+64 9 375 4101	
Web-сайт службы технической поддержки	http://service.symantec.co.nz	
Техническая поддержка по плану Gold	0800 174 045	gold.nz@symantec.com
Информация о контрактах технической поддержки	0800 445 450	contractsadmin@symantec.com

Сингапур

Symantec Singapore
3 Phillip Street
#17-00 & #19-00 Commerce Point
Singapore 048693

Основной номер телефона	+65 6239 2000
Факс	+65 6239 2001
Техническая поддержка	+65 6239 2099
Web-сайт	http://www.symantec.com.sg

Тайвань

Symantec Taiwan
2F-7, No.188 Sec.5
Nanjing E. Rd.,
105 Taipei
Taiwan

Основной номер телефона	+886 2 8761 5800
Техническая поддержка для организаций	+886 2 8761 5800
Факс	+886 2 2742 2838
Web-сайт	http://www.symantec.com.tw

Мы сделали все возможное, чтобы представленная здесь информация была полной и точной. Тем не менее, содержащаяся в настоящем документе информация может быть изменена безо всякого уведомления. Корпорация Symantec оставляет за собой право на внесение таких изменений без предварительного уведомления.